# CSEC640 IA2: Browser and IDPS Security Analysis

Megan Bell

University of Maryland University College

March 31, 2017

## Author**'s** Note

This paper was prepared for CSEC 640 Monitoring, Auditing, Intrusion Detection, Intrusion Prevention, and Penetration Testing, taught by Professor Steven Rigby.

Table of Contents

## IA2: Cyber Attack and Intrusion Prevention

### Introduction

Internet technologies have evolved to an era of ubiquitous computing where resources are available on demand anywhere and anytime. Wireless technologies provided reach; data centers provide intermediary points of application delivery, processing and storage; and web browser technologies serves as the interface for user access. This transformation of original Internet technologies may be observed in Google's software model where services are available on demand through a browser, and no software updates are required. While organizations and end-users enjoy the benefits, two important and related channels of security create risk for digital assets and reliable and accessible Internet use. One primary of channel of security is the Internet web browser, which is a lynchpin to user and endpoint device security. The second channel is network protection mechanisms that monitor and filter potential threats. With the Internet and browsers now serving as "web as platform" as illustrated in Appendix A Figure A1, curtailing browser and data channel risk is paramount to maintain future use of Internet technologies such as web applications (O'Reilly, 2005).

This paper examines issues, problems, and potential solutions for the areas of browser technology and network intrusion prevention and detection. Browsers are the primary unit of trust for delivering web application content. Underlying vulnerabilities stem from user behaviors and lagging browser security. Solutions require better backend trust, security for browser support resources, and controls to reduce user risk. Next, network intrusion protection and prevention technologies require ongoing attention and technological advancement. Cloud and wireless

technologies have contributed to critical gaps in organizational ability to monitor and thwart potential network data risks. It may be that full cloud embracement is necessary for solutions to improve visibility into network data and to increase issue detection.

## Paper 1: Browser attacks and protection

### Overview

A 2008 analysis by the Web Application Security Consortium ([WASC], 2008) of 12,186 websites with 97,554 detected vulnerabilities indicated that cross-site scripting (XSS), information leakage, and SQL injection were the most common vulnerabilities as presented in Appendix B Figure B1. While the majority of vulnerabilities were identified as server-side exposures, XSS was the predominant client-side vulnerability. Even though XSS is the most significant source of client-side vulnerabilities from Internet browser use, other vulnerabilities also create exposure risks for end-users and could be exploited to compromise the confidentiality and integrity of information resources as well as the availability to browser or device resources. Appendix B Table B2 contains a compiled listing of browser vulnerabilities. While browser security risks are discussed with respect to exploitable vulnerabilities such as JavaScript, browser risks more broadly stem from user actions, insecure browsers, and software coding practices.

### Underlying Sources of Risk

#### Users Perceive Risk Differently.

Research suggests that users practice computer security relative to personal gain (Herley, 2009). Specifically, the time and complexity required to accomplish better security is compared

to the perceived risk of personal compromise (e.g., theft from a bank account) and perceived need for protection (Schneier, 2008). Security is about prevention to reduce the possibility of negative consequences and not to lock out intruders (Schneier, 2003). As an example, a landmark password research study evaluated user habits across 544,960 browser client toolbars that collected several months of data on Internet browsing (Florencio & Herley, 2007). The study found that the average user had about 25 accounts requiring passwords and entered an average of 8 passwords per day. In managing password-requiring user accounts, users tended to rely on lowercase passwords where password complexity was required. Users also relied on persistent logins where the length of time between new logins ranged from 4 to 9 days. Users practiced security, but not necessarily to the extent desired by security professionals. Password practices appeared commensurate with compliance rather than the perceived need for security. In another study that evaluated security respective to users' Internet tasks and user perception of security, users ranked familiar tasks as lower risk, even though notable risks may have existed (Byrne, Dvorak, Peters, Ray, Howe, & Sanchez, 2016). Security was secondary to task completion.

**Browsers Evolving Faster than Security.**

The rise of Web 2.0 and rapid user adoption has contributed to the development of browser technology for the delivery of real-time applications such as Web video conferencing. Ideally, security should be embedded into the browser and throughout the Internet's supporting architecture (Alvestrand, 2012). This framework should create a hierarchy of trust that originates with the browser, and continues systemically with additional layers of security

(Rescorla, 2013). Unfortunately, protocols for browser security standards have evolved but seem to outpace security design and deployment.

As evidence of further advancement, web browser technology has contributed to the proliferation of broader mobile and cloud computing technologies and services. A key driver to web browser technology's influence is the hypertext markup language (HTML) for the display of content within a browser's interface. The most current version of HTML5 is used across most devices that employ web browser technology. HTML5 delivers functionality such as touch screen interactions, dynamic graphics, and mobile device efficiency (Xinogalos, Psannis, & Sifaleras, 2012). In addition, HTML5 has advantages over its predecessors in the use of storage such as local session storage (West & Pulimood, 2012). This could increase user device risk.

The proliferation of web browsers and HTML5 technologies have escalated the universe of potential security vulnerability channels and other risks. These risks build on traditional web browser security risks such as plug-ins software (Starov & Nikiforakis, 2017). Plug-ins and certain toolbars are not browser native technology and introduce potentially vulnerable code to a browser. For example, Adobe Flash is associated with numerous browser exploits (Wressnegger, Yamaguchi, Arp, & Rieck, 2015). As discussed earlier, features such as increased local storage of sensitive data browsers could increase the possibility of browsers becoming attack targets. Risks could be compounded through underlying technologies that deploy HTML5 such as asynchronous JavaScript and XML (AJAX) (Johnson, Conrad, Misenar, 2016). This includes an increased attack surface for XSS vulnerabilities. The ambiguity of HTML5 risks may exist within customized coding constructs or evolving backend techniques.

Finally, newer attack vectors may leverage web browser technology such as JavaScript for device-level attacks. One example is the recent demonstration of an address space layout randomization (ASLR) attack in which memory locations associated with web browser use are located and exploited (Gras, Razavi, Bosman, Bos, & Giuffrida, 2017). Ideally, ASLR should protect computer memory from such attacks. However, security researchers discovered how to reverse engineer memory patterns while using a browser-related JavaScript timer. Previously, browser vendors disabled JavaScript timer functionality.

## Solutions

### Establish Broader Backend Trust by Default

Web trust is founded on the same origin policy, which states that programmatic code and content must originate from a single source rather than multiple sources (Johnson, Conrad, & Misenar, 2016). Without same origin, web applications could potentially attack each other or a client within the same browser. Distributed computing and the expansion of Internet services have diversified the backend resources that deliver browser content. With this change, backend technologies have created alternative trajectories for the creation, dissemination, and management of browser content. Also, trust is often embedded at specific front-end points such as a website login page rather than being browser-ubiquitous. As Internet technology advances, models of trust based on same origin policy should evolve to include broader backend trust to ensure all points and channels of trust can systemically demonstrate trust across a distributed ecosystem (Tulasidas, Mackay, Hudson, & Balachandran, 2017).

**Improve Security Requirements for Browser Support Resources.**

Browsers rely on external software for extended use such as Java and as previously highlighted, Adobe Flash. This supporting software has become pivotal for extended use of web browser for business applications (Erbeschloe, 2015). The downfall is that browser technologies have advanced independently of supporting software, and have worsened the security divide between browsers and supporting software. Some security researchers indicate disabling support software to achieve better security (Herzberg & Jbara, 2008). This avoids security as an issue but disables important user functionality. Other proposals provide for independent security remediation of supporting resources such as Gordon for Adobe Flash implementations that fix and application but not the browser (Wressnegger, Yamaguchi, Arp, & Rieck, 2015). Improved browser security would be achieved if browsers had better native security and supporting software with commensurate security protection that was not developer-dependent. Security should be supported within the browser first and web applications second. Then, as a validation of better security, web applications should employ standardized adversarial testing practices in vulnerability assessment to provide additional security assurance (Pokharel, Choo, & Liu, 2017). This could then result in a default standard of be a better overall security (Wadkar, Mishra, & Dixit, 2017).

**Advance Access Controls (AC).**

Users practice security when required, and security should account for user psychology rather than attempt excessive change for user habits. Two avenues of protection against user behaviors are authentication and access controls. Authentication and access control models are not new, but there is room for improvement given human propensities for weaker security practices. Several authentication models have been adapted for web applications with tools such as two-

factor authentication. The potential improvement for better authentication resides with better adoption of more advanced technologies and browsers that support stronger HTTP security practices. A study by Acker, Hausknecht, and Sabelfeld (2017) found that at least 32% of login pages for the top 100,000 Internet domains can be compromised by man-in-the-middle (MiTM) attacks due to lack of better authentication security. If organizations update their authentication with adherence to strong HTTP protocol practices, user risk from MiTM practices could be greatly mitigated. As a caveat, browsers must also enforce strong HTTP security such HTTP Public Key Pinning (HPKP) and HTTP Strict Transport Security (HSTS).

AC has not experienced the same security evolution as authentication. Unauthorized access is considered a significant source of asset loss, and better AC models are identified as a means to remediate unauthorized access risk (Joshi, Aref, Ghafoor, & Spafford, 2001). Existing AC models such as role-based access control (RBAC) have been documented as adaptive to web applications. RBAC enables strong security practices such as least privilege and separation of duties. RBAC can also be centrally managed and implemented through group policies. Newer AC models such as task-based access control (TBAC) address advances in workflow methodologies introduced by web applications and enforce security based on how users work.

## Paper 2: Network Intrusion Prevention, Detection and Event Analytics

### Overview: Protecting the Entire Network

The rapid growth in cloud computing architecture models and service deployment options has shifted IT resources from traditionally closed networks to distributed networks where organizations own content but not computing resources (Zhang, Cheng, & Boutaba, 2010). Cloud

providers may be infrastructure or service providers with infrastructure, application, or service offerings as illustrated in Appendix C Figure C1. Organizational choice of cloud provider is based on business and computing requirements, but software-as-a-service (SaaS) plays a predominant role with the five biggest cloud services being web hosting, file storage business applications, email, and desktop applications (Pritchard, 2015). With more than half of businesses using the cloud, a majority of organizations balance a blended network footprint of traditional and cloud IT infrastructures.

Determining the best approach and the use of intrusion detection system (IDS) and intrusion protection systems (IPS) is dependent on control of information infrastructure and value of information assets. It should be noted that best approach assumes that infrastructure control is stronger with an internal network than cloud infrastructure. Also, it is assumed that information assets must be qualified by the owner organization. With assumptions in mind, an organization's control of internal network and information systems enable stronger deployment of IDS and IPS to monitor network traffic and respond to suspicious activity. Internal networks can be configured with centralized controls and points of trust such as Microsoft Active Directory Services (Kušen & Strembeck, 2017).

The degree of control over cloud infrastructure depends on the type of cloud deployment and services provided by a respective cloud provider. Cloud technologies reside in data centers with sophisticated network architecture that exists in core, aggregation, and access layers as observed in Appendix C Figure C2 (Zhang, Cheng, & Boutaba, 2010). Cloud providers often have substantial control and ownership of security across the cloud-infrastructure. This includes design

and deployment of IDS and IPS resources. An organization must respectively define its security roles and responsibilities with a specific cloud provider, but understand that cloud providers may not fully share network architecture, security information, or security event analytics. Organizations may be limited to network perimeter controls, audit reports, and legal contracts to establish and assure network security. Given the potential uncertainty, organizations must balance differing environments where cloud security risks require adjustment given the limits of cloud provider control.

## Specific Issues

### Cloud's Centralized Risks: Denial of Service (DoS) and DNS

In early 2016, Internet services provider Dyn experienced a distributed denial of service attack (DDoS) attack that resulted in significant disruption of Internet services to many large organizations such as Netflix and The New York Times (Newman, 2016). Organizations such as Akamai and Flashpoint provided external intrusion detection warnings with early detection of attack traffic, and Dyn had certain capabilities to partially thwart the attack. However, the breadth and extent of the attack interrupted network availability for several hours. While financial costs of the attack were not released, the financial impact of DDoS attacks has been estimated to be as much as $400,000 for a single attack (Somani, Gaur, Sanghi, Conti, and Buyya, 2015). Not all organizations have external IDS assistance and early threat detection.

The Dyn attack highlights two risks that could impact all organizations relying on cloud services. First, organizations require robust Internet connectivity to access and utilize cloud resources. When Internet availability is blocked, interrupted, or suspended, an organization may

not have alternative access to information resources such as a backup service. Second, Dyn is a Domain Name Services (DNS) provider and maintains DNS address resolution for mapping hosts and domain names. Loss of DNS is loss of access to computing resources. The issue for IPS is early interruption of DDoS attacks possible advanced remediation for DNS data.

**Wirelesss Network Risk.**

Growth in wireless network communications has outpaced the commensurate advances in IDS and IPS systems for wireless communications. Wireless networks may be integrated into traditional wired network infrastructures with IDP and IPS capabilities, but can also be implemented as flexible, ad-hoc networks with no monitoring. The potential lack of monitoring is a cornerstone of distrust with wireless networking. Also, the potentially dynamic nature of wireless communications may create substantial and unknown security risks for an organization. Further, traditional IDS and IPS systems were built for wired network protocols and not for newer wireless communications types and protocols. This perspective may be observed by examining the Payment Card Industry (PCI), which defines and enforces requirements for processing and storing payment card data (e.g., Visa). PCI requires organizations in its customer and service provider ecosystem to protect credit card data with strong layered security programs that include firewalls and intrusion detection prevention systems (IDPS) (Payment Card Industry Security Standards Council [PCI-SSC], 2009). However, PCI includes the additional requirement of occasionally scanning for "rogue" wireless access points as part of compliance with PCI's data security standards (DSS).

Wireless networks encompass several technologies and standards (Vacca, 2013). Cellular

and 802.11 wireless networks have existed for many years and expectantly, have directionally better understood security risks for wirelesss versus newer protocols. This includes short-range communications technologies such as radio frequency identification (RFID) and Bluetooth. RFID has been deployed for a number of uses such as asset management, physical security, and tracking marathon runners (Want, 2006). Bluetooth is an important short-range communications channel for connecting locally situated devices. RFID and Bluetooth carry significant intrusion detection risks such as the ability to identify signal sources and manipulate communications channels. For example, vulnerabilities such as Bluetooth device MAC address discovery have been exploited through radio-based frames analysis of the wireless signals (O'Connor, 2008). After obtaining a MAC address, it is possible to enumerate and identify exploits. To some extent, these vulnerabilities result form immaturity in technology standards and implementation. In this context, IDS and IPS solutions for wireless networks are not mature with respect to device detection, suspicious pattern recognition, and the ability to enforce control.

**Big Data.**

Big data is another emerging vector of security risk. Big data refers to massive data collections stored from the generation, collection, and processing of data. Many big data systems are cloud-native and controlled by cloud providers. While organizations with big data may secure big data with their information security programs for cloud environments, a substantial security gap exists within monitoring the network flow of big data communications and understanding the security risks of big data applications (Zuech, Khoshgoftaar, & Wald, 2015).

### Proliferation of Endpoints, Protocols and Content Types.

Distributed computing has shifted organizations away from highly normalized environments with predictable network traffic patterns to a plethora of endpoint devices with differing patterns of network traffic and content types. Modern IDS implementations must account for the shift in endpoint diversity with less predictable network traffic patterns and difficulty in discernment of anomalous and suspicious activity (Desai, 2002). This includes the detection of network reconnaissance, IP spoofing, DoS, leakage of sensitive information, and buffer overflows. For larger organizations, the challenge is three-fold. First, effective IDS and IPS are founded on a known baseline of information security. The diversity of devices and network traffic sources and types may impede development of effective baselines. Second, IDS and IPS systems must be adaptable for new device, protocols, and content. Third, there should be greater focus in defining and monitoring the context of misuse (O'Connor, 2008). Understanding extremes of typical network traffic and instances of misuse provide insight for effective IDS and IPS implementations.

## Solutions

### Leveraging Cloud and Big Data to Better Security

While cloud, big data, and endpoint device proliferation may seemingly limit security, there is actually greater opportunity to create big data IDS for blended network security defense. One benefit of big data capabilities is the availability of data architectures and tools that normalize and absorb potentially irreconcilable data sources (Zuech, Khoshgoftaar, & Wald, 2015). Data inputs could include existing security information and event management (SIEM) and IDS

systems as well as data feeds from cloud IDS and other log sources. Data normalization would result from more efficient processing and transmission of log data such as use of MapReduce technology (Thota, Manogaran, Lopez, & Vijayakumar, 2017). The benefit of normalization is visibility across a broader information resoureces. Further, IDS systems can be automated for event and alert analytics as well as connecting to IPS. Security monitoring could even be adapted for monitoring big data streams where central management includes security verification at a highly granular level for real-time data use (Puthal, Nepal, Ranjan, & Chen, 2017).

**Upgrading Network Protections—Particularly for Wireless**

Where network communications or cloud services are governed by contract, contract requirements should include provisions for network traffic monitoring and Quality of Service (QoS) (de Carvalho, de Castro Andrade, de Castro, Coutinho, & Agoulmine, 2017). Network traffic monitoring could include DoS threat detection and mitigation services with the use of products such as Securi CloudProxy.

Organizations may also consider the services of Security Operations Centers (SOCs) to enhance IDS and IPS capabilities (Koulouris, Casassa Mont, & Arnell, 2017). Many SOCs now provide comprehensive networks security with specialized software and analytics. This approach to security could also address the security gaps in wired IDS and IPS systems (Zhang & Lee, 2009). Newer wireless technologies such as signal processing for granular threat detection may also be available through SOCs or other specialized security service providers (Edwards, 2017).

Finally, layered security protocols are recommended for securing the diversity of wireless communications, and the method specific implementation of security depends on the type of

wireless communication (Vacca, 2013). This may include supplemental pen testing and IDS capabilities tailored to wireless protocols and attack patterns such as evesdropping. Also, with respect to browser technologies, layered security protocols close the gap in security associated with data transmission and point-to-point data transitions between differing networks.

**References**

Alvestrand, H. (2012). Overview: Real time protocols for browser-based applications (Working draft). IETF Trust Network Working Group. Retrieved on March 29, 2017, from https://tools.ietf.org/id/draft-ietf-rtcweb-overview-04.txt

Byrne, Z. S., Dvorak, K. J., Peters, J. M., Ray, I., Howe, A., & Sanchez, D. (2016). From the user's perspective: Perceptions of risk relative to benefit associated with using the Internet. *Computers in Human Behavior*, *59*, 456-468.

de Carvalho, C. A. B., de Castro Andrade, R. M., de Castro, M. F., Coutinho, E. F., & Agoulmine, N. (2017). State of the art and challenges of security SLA for cloud computing. Computers & Electrical Engineering.

Desai, M. D. (2002). Distributed intrusion detection (Doctoral dissertation, Indian Institute of Technology, Bombay Mumbai).

Edwards, J. (2017). Stepping up security with signal processing: Innovative tools and approaches address threats on multiple fronts [Special Reports]. IEEE Signal Processing Magazine, 34(2), 14-17.

Erbschloe, M. (2015). Business applications of Java. Research Starters: Business (Online Edition)

Florencio, D., & Herley, C. (2007, May). A large-scale study of web password habits. In *Proceedings of the 16th international conference on World Wide Web* (pp. 657-666). ACM.

Gras, B., Razavi, K., Bosman, E., Bos, H., & Giuffrida, C. (2017). ASLR on the line: Practical Ccche attacks on the MMU. *NDSS (Feb. 2017)*.

Herley, C. (2009, September). So long, and no thanks for the externalities: the rational rejection of security advice by users. In *Proceedings of the 2009 workshop on New security paradigms workshop* (pp. 133-144). ACM.

Herzberg, A., & Jbara, A. (2008). Security and identification indicators for browsers against spoofing and phishing attacks. *ACM Transactions on Internet Technology (TOIT)*, *8*(4), 16.

Joshi, J. B., Aref, W. G., Ghafoor, A., & Spafford, E. H. (2001). Security models for web-based applications. Communications of the ACM, 44(2), 38-44.

Johnson, K., Conrad, E., Misenar, S. (2016). SEC 542 Web penetration testing and ethical hacking: Introduction and Information Gathering. The SANS Institute.

Koulouris, T., Casassa Mont, M., & Arnell, S. (2017). SDN4S: Software Defined Networking for Security.

Koussa, S. et al. (2013). Static analysis technologies evaluation criteria. The Web Application Security Consortium. Retrieved March 29, 2017, from http://projects.webappsec.org/w/file/66107997/SATEC_Manual-02.pdf

Kušen, E., & Strembeck, M. (2017). Security-related Research in Ubiquitous Computing--Results of a Systematic Literature Review. arXiv preprint arXiv:1701.00773.

Newman, L. H. (2016, October 21). What we know about Friday's massive East Coast Internet outage. Wired. Retrieved from https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/

O'Connor, T. (2008). Bluetooth Intrusion Detection (Graduate thesis). Retrieved on March 30, 2017, from https://repository.lib.ncsu.edu/bitstream/handle/1840.16/235/etd.pdf?sequence=1&isAllowed=y

Payment Card Industry Security Standards Council (PCI-SSC). (2009, July). Data Security Standard (DSS) information supplement: PCI DSS wireless guideline. Retrieved from https://www.pcisecuritystandards.org/pdfs/PCI_DSS_Wireless_Guidelines.pdf

Pokharel, S., Choo, K. K. R., & Liu, J. (2017). Mobile cloud security: An adversary model for lightweight browser security. Computer Standards & Interfaces, 49, 71-78.

Pritchard, S. (2015). Preparing for next-generation cloud: Lessons learned and insights shared. *He Economist Intelligence Unit Limited*. Retrieved January 29, 2017, from https://www.eiuperspectives.economist.com/sites/default/files/EIU_Hitachi_Preparing%20for%20next%20generation%20cloud%20PDF.pdf

Puthal, D., Nepal, S., Ranjan, R., & Chen, J. (2017). A dynamic prime number based efficient security mechanism for big sensing data streams. Journal of Computer and System Sciences, 83(1), 22-42.

Rescorla, E. (2013). WebRTC security architecture (Working draft). IETF Trust Network Working Group. Retrieved on March 29, 2017, from https://tools.ietf.org/id/draft-ietf-rtcweb-security-arch-07.txt

Schneier, B. (2003). Beyond fear: Thinking sensibly about security in an uncertain world. Springer Science & Business Media.

Schneier, B. (2008, June). The psychology of security. In *International Conference on Cryptology in Africa* (pp. 50-79). Springer Berlin Heidelberg.

Somani, G., Gaur, M. S., Sanghi, D., Conti, M., & Buyya, R. (2015). DDoS Attacks in cloud computing: issues, taxonomy, and future directions. Retrieved from https://arxiv.org/pdf/1512.08187.pdf

Starov, O., & Nikiforakis, N. (2017). Extended tracking Powers: Measuring the privacy diffusion enabled by browser extensions. In Proceedings of the 26th International Conference on World Wide Web, WWW (pp. 3-7).

Thota, C., Manogaran, G., Lopez, D., & Vijayakumar, V. (2017). Big data security framework for distributed cloud data centers. In Cybersecurity Breaches and Issues Surrounding Online Threat Protection (pp. 288-310). IGI Global.

Tulasidas, S., Mackay, R., Hudson, C., & Balachandran, W. (2017). Security framework for managing data security within point of care tests. Journal of Software Engineering and Applications, 10(02), 174.

Vacca, J. R. (2013). Computer and information security handbook (Second ed.). Amsterdam: Elsevier.

Wadkar, H. S., Mishra, A., & Dixit, A. M. (2017). Framework to Secure Browser Using Configuration Analysis. International Journal of Information Security and Privacy (IJISP), 11(2), 49-63.

Want, R. (2006). An introduction to RFID technology. *IEEE pervasive computing*, *5*(1), 25-33.

Web Application Security Consortium (WASC). (2007). Web application security statistics project 2007. Retrieved March 29, 2017, from http://projects.webappsec.org/f/wasc_wass_2007.pdf

Web Application Security Consortium (WASC). (2008). Web application security statistics project 2008. Retrieved March 29, 2017, from http://projects.webappsec.org/w/page/13246989/Web%20Application%20Security%20Statistics

Wressnegger, C., Yamaguchi, F., Arp, D., & Rieck, K. (2015). Analyzing and detecting flash-based malware using lightweight multi-path exploration. *University of Göttingen, Germany*.

West, W., & Pulimood, S. M. (2012). Analysis of privacy and security in HTML5 web storage. *Journal of Computing Sciences in Colleges*, *27*(3), 80-87.

Xinogalos, S., Psannis, K. E., & Sifaleras, A. (2012, September). Recent advances delivered by HTML 5 in mobile cloud computing applications: a survey. In *Proceedings of the Fifth Balkan Conference in Informatics* (pp. 199-204). ACM.

Zhang, Q., Cheng, L., & Boutaba, R. (2010). Cloud computing: state-of-the-art and research challenges. *Journal of internet services and applications*, *1*(1), 7-18.

Zuech, R., Khoshgoftaar, T. M., & Wald, R. (2015). Intrusion detection and big heterogeneous data: a survey. *Journal of Big Data*, *2*(1), 3.

## Appendix A

Web Applications

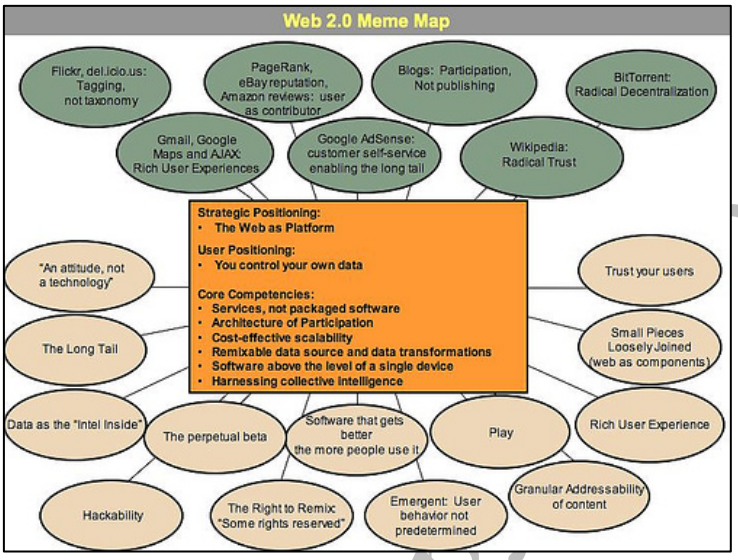


Figure A1. "Meme" map of Web 2.0 descriptors and competencies. Reprinted from "What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software", by O'Reilly, Tim, 2005, Retrieved from http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html. Copyright 2005 O'Reilly Media.

## Appendix B

WASC Security Statistics Project 2007 and 2008

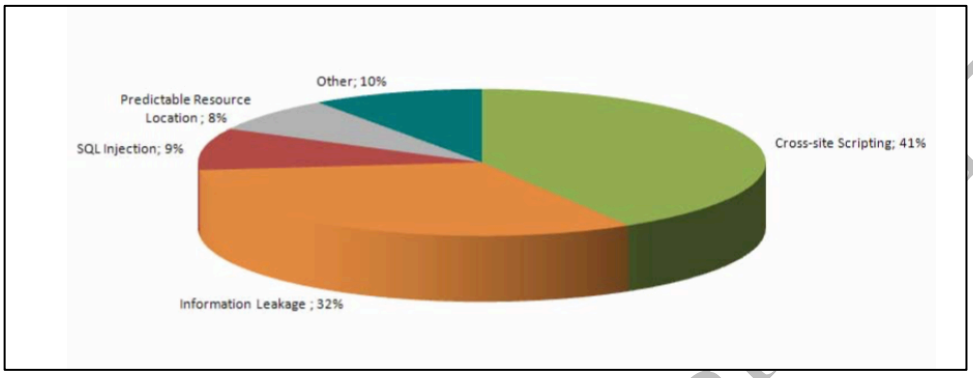


Figure B1. Vulnerability frequency by type from analysis of 32,717 sites and 69,476 vulnerabilities. Reprinted from "Web Application Security Statistics Project 2007", by Web Application Security Consortium (WASC), 2007, retrieved from http://projects.webappsec.org/f/wasc_wass_2007.pdf. Copyright 2017 by WASC.

| Table B2. Summary of Browser Vulnerabilities | |
|---|---|
| Vulnerability Type | Description |
| Content Spoofing | Injection of content to a browser that alters the original content of a web page. Also referred to as virtual defacement. The source server's content is not altered. |
| Cross-Site Request Forgery (CSRF) | This attack results in an end-user submitting unwanted requests to a web application where the user is actively authenticated. An |

| Table B2. Summary of Browser Vulnerabilities | |
|---|---|
| Vulnerability Type | Description |
| | example attack is where an attacker provides a malicious hyperlink to a victim, and the victim clicks on the link. After the click, the website associated with the link processes the attacker's link using the end user's active session. |
| Cross-Site Scripting (XSS) | XSS refers to injection of malicious software code into a web application. While XSS vulnerabilities may exist on the web server and client browser, this paper addresses client-side XSS attacks. XSS vulnerabilities result from coding flaws in HTML pages that create entry points into page elements such as form fields to insert malicious code. When a user interacts with the page element where malicious code exists, the code executes. Successful attacks may have a range of outcomes such as downloading malware or web cache poisoning. XSS vulnerabilities also violate the trust relationship between an end-user and a browser in use. |
| HTTP Request/ Response Splitting | HTTP Splitting occurs due to flaws in servers-side processing of user data in HTTP headers. HTTP headers use character |

| Table B2. Summary of Browser Vulnerabilities | |
|---|---|
| Vulnerability Type | Description |
| | elements such as line breaks and carriage returns to identify the end of a header request. When these characters are not properly placed or are missing, an HTTP splitting vulnerability is created. Splitting refers the ability to manipulate the missing end of HTTP header characters to divide a single HTTP request and response communication into two HTTP request and response communications. HTTP Response Splitting is the primary attack type deployed against browsers. This attack is a vehicle to execute other attacks such as XSS or browser cache poisoning. |
| HTTP Request / Response Smuggling | This type of attack involves the use of proxy server intermediaries that exist between web servers and browsers. Similar to HTTP Splitting, HTTP Smuggling is a vehicle for conducting other attacks such as web-cache poisoning or security bypass. HTTP Smuggling attacks involve manipulation of the HTTP protocol due to lack of strict standards in parsing and interpreting HTTP headers. |
| Insufficient Transport Layer Protection | This particular vulnerability refers to manipulation of traffic between endpoints |

| Table B2. Summary of Browser Vulnerabilities | |
|---|---|
| Vulnerability Type | Description |
| | such as a web server and a browser. When there is weak or lacking security in web data traffic such as lack of encryption or authentication, there is exposure risk to manipulation of web data traffic. These vulnerabilities may lead to exploitation of other vulnerabilities such as CSRF. |
| Cross-Zone and Cross-Domain Vulnerabilities | Browsers were developed with a security model based on same origin policy, which states that web pages coming from the same protocol, host, and port have the same origin. A change in one of the three variables is a change in origin and violation of same origin. Deployment of same origin policy varies by browser, and a web application may have backend deployment that bypasses same origin policy. Cross-zone and cross-domain vulnerabilities exist with these backend server modifications and could provide possible access for attack types such as XSS. |
| Plug-in Vulnerabilities | Plug-ins are software applications that integrate additional functionality into browsers. Plug-ins may contain flaws in software design and configuration that |

| Table B2. Summary of Browser Vulnerabilities | |
|---|---|
| Vulnerability Type | Description |
| | could lead to successful attacks such as malicious code injection or buffer overflow. |
| URL Redirectors | URL redirection is a fundamental tool in the backend management of website traffic. Within a web browser, URL redirects become vulnerable when an attacker is able to input a malicious URL that redirects a victim to an alternative location or results in download of malicious data. URL redirection may be used in client-side attacks such as XSS attacks. |

Table B2. Vulnerability compilation for client-side browser vulnerabilities. Compiled from "Web Application Security Statistics Project 2007", by Web Application Security Consortium (WASC), 2007, retrieved from http://projects.webappsec.org/f/wasc_wass_2007.pdf. Copyright 2017 by WASC.

## Appendix C

Cloud Computing Models

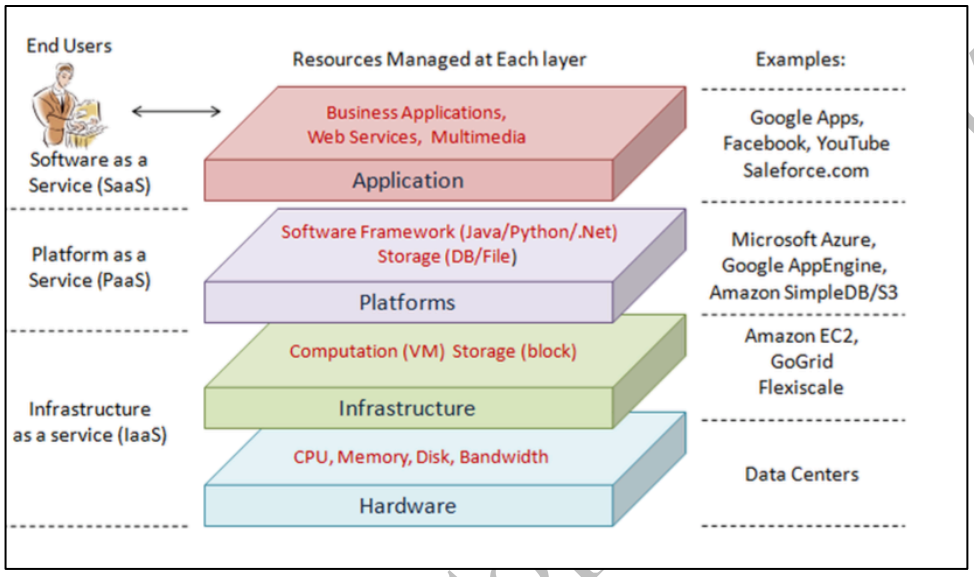


Figure C1. Cloud computing models. Reprinted from "Cloud Computing: State-of-the-Art and Research Challenges ", by Q. Zhang, L. Cheng, L., & R. Boutaba, 2010, *Journal of Internet Services and Applications*, *1*(1), 7-18, retrieved from 10.1007/s13174-010-0007-6. Copyright 2017 by Springer.

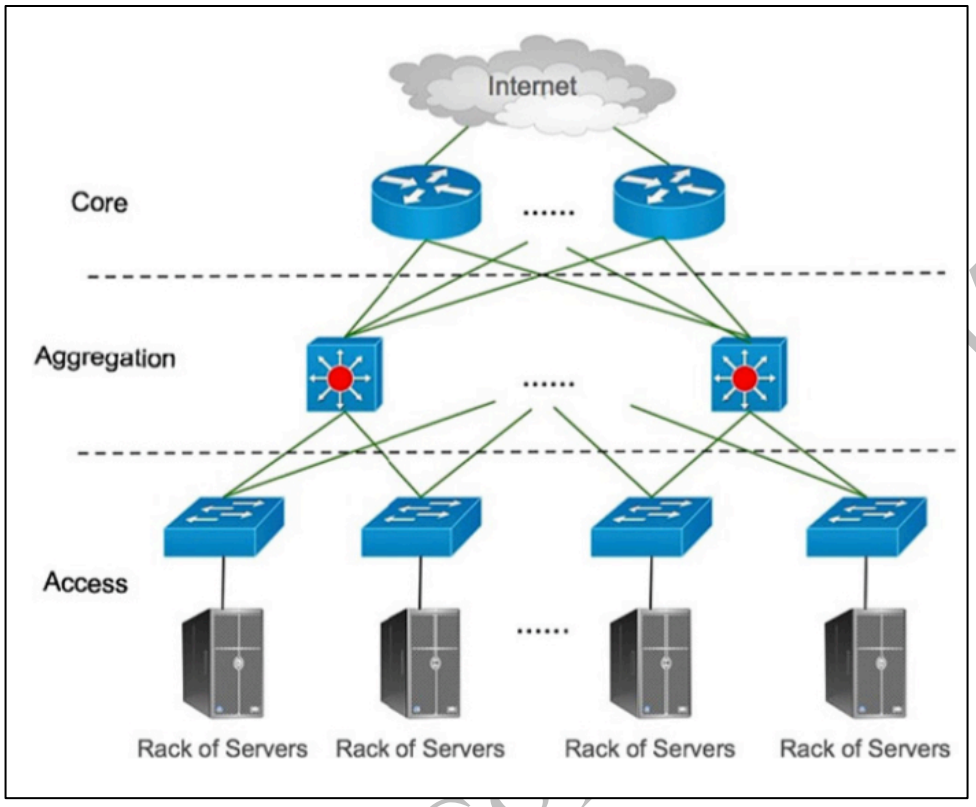


Figure C2. Illustration of layered data center network. Reprinted from "Cloud Computing: State-of-the-Art and Research Challenges ", by Q. Zhang, L. Cheng, L., & R. Boutaba, 2010, J*ournal of Internet Services and Applications*, *1*(1), 7-18, retrieved from 10.1007/s13174-010-0007-6. Copyright 2017 by Springer.