Why EndPoint Security Is Must

Critical Reflection

Soubhik Chakraborty

Bentley University

CS607 Cyber Security

Prof. David Yates

Sep' 2022

Author Note

After working in the IT industry for more than two decades, having developed various infrastructural products and deploying them at web scale, including FBI & Indian defense, I intend to elaborate on the need for endpoint security (end user device security) from a more practical standpoint. Mainly start with how the industry has tried enough just to secure the servers alone but still left wanting to completely secure against vulnerabilities, thus justifying why PII (Personal Identification Information) must be exposed in a controlled and responsible way to provide end-to-end secured access.

Abstract

Enterprise data centers have evolved drastically since the last decade of the 20th century till present day, both in terms of computing capacity and need for information exchange. As the enterprise deployments evolved from monolith mini mainframes to rack servers to commodity hardware clustering (distributed computing) to server & network virtualization to cloud computing, the need to service more and more users instantly and securely is ever growing, and so does the data availability real-time. With this ever-expansion of the interweb and the rise of the users' edge devices, interoperating continuously round the clock around the world, it has become virtually impossible to keep track of the network traffic flow between server and client by just monitoring and safeguarding the server side alone (assets and network). In this analysis I will enumerate various **layers of security** (Climer & Khan, 2020) (phoenixNAP, 2019) measures taken in the most modern enterprise deployments and walk through some general hacks and some exotic ways that indicate how these sophisticated measures (*Is Your Server Secure Enough?*, 2017) (Ridgeback, 2018) can still be toyed with, bypassed and compromised undermining the overall server side security. The biggest opposite force of cybersecurity is budgetary constraints and "ease of use". Security implementations must constantly balance between seamless access to the "good" actors while accurately identifying the "bad" actors, leaning too much on either side (too much or too less of security) has business implications in both the situations. Lastly, I will point out how end-point security compliments the server side measures, thus helping to reduce the attack vectors drastically, enabling us to architect a more robust system without compromising on ease of use of the services offered.

Server Security in depth, its insufficiency and further advancements

There are many aspects that are under consideration when it comes to securing a server. Enterprise deployments have many layers of security, right from datacenter choice of location to application services exposed to end users, but despite all the protective measures we are constantly faced with security breaches more often than we would expect it to happen. In this paper, I will walk through various aspects that are in play for securing a server, still falling short on constantly evolving threat vectors, and thus make a case for identifying each clients' device(s) as a necessity trading off user privacy to some extent.

WHAT IS SERVER SECURITY

There are many dimensions to server security and each topic below deserves separate volumes. To focus on an overview, for each topic is mentioned with several standards that enumerate detailed guidelines. These are followed at various degrees of compliance by the enterprises according to their IT budget, technology adoption and ability to hire skill sets.

Physical Security: Datacenter and Location Security

While choosing the location of a datacenter, understanding the cyber law of the country, for example legislations like (*Cybersecurity Legislation 2021*, 2022), (*US and EU Data Localization and Data Transfer Restriction Laws*, 2021), (*44 USC CHAPTER 35, SUBCHAPTER II: INFORMATION SECURITY*, n.d.), (*Cybersecurity Unit - Criminal Division*, n.d.), (*European Parliament and of the Council of 6 July 2016*, n.d.) is the first priority.

Next comes certification of the data center such as CISA (*Cybersecurity and Physical Security Convergence*, n.d.) and many others like FISMA, FedRAMP, HIPAA certifications. Then there is following of SEC guidelines and state laws (Baadsgaard, 2021)

Building construction standards for data centers are very different and largely depend on uptime and intrusion resistance levels offered (*ECS Data Center Have Best-In-Class Physical Security*

Standards – All About Tier 4 Data Center, n.d.). A more comprehensive list of things to consider can be found in ***Design and Build a Data Center***. (Bigelow, 2022). Staffing, Power Grid redundancy, Rodent, Water leakage and Fire resistance, ASHRAE standards for heat management, Natural Disaster and physical attacks like bombings that can destroy the buildings are all part of physical security and deserves topic of its own.

Assuming the above aspects are covered, let us turn our attention to another aspect of physical security which is hardware security.

Physical Security: Hardware Security

For physical server security there are many aspects like Over allocation of floor space in a datacenter, caged racks for servers, single entry/exit system, and also adhering to various NIST guidelines like (*IT Asset Management: NIST Publishes Cybersecurity Practice Guide, Special Publication 1800-5 | NIST*, 2018), Hardware Security Thorough Supply Chain Assurance | NIST (Obeng, 2016).

Physical Network security also has many aspects. For example securing network devices such as routers, switches, LAN & WAN cabling are imperative. Secured connectivity with other externally hosted network elements like wireless towers, radio frequency band exclusivity is more of infrastructure security that requires consideration while designing data centers and inter datacenter high speed connectivity. Few known standards that internet providers follow are NIST (*Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1*, 2018), GSMA, 3GPP, ETSI. Furthermore, physical network isolation for critical services of an enterprise are deployed within data centers and access control protocols are generally more stringent than common areas.

Remote management of these server/network deployments is another tricky area often planned poorly until a couple of years back. This attack vector is heavily used in the last decades, which is covered in more details later.

Software Security: Deployment Strategies

On Premise Deployment

For IT focused enterprises this deployment is preferred but often partially adhered to various standards. Nevertheless, basic compliance is achieved for the following aspects.

a) Operating System hardening based on *Guide to General Server Security* (Tracy et al., n.d.) are provided by providers like CIS

b) Network security guidelines are laid down by standards like (*Cyber and Network Security | NIST*, n.d.).

c) Kernel hardening (Brown, 2016) is another aspect in server deployments on linux. Various hardware manufacturers offer UEFI secure boot (*Secure Boot Overview*, 2021) which essentially safeguards against OS hijacking, root kit installations, or usage of trusted firmwares often provided by other vendors.

d) System hardening (*What Is Systems Hardening?*, n.d.) involves many other aspects other than just OS hardening like default password erasure, lack of privileges for critical access control, user profile creation restrictions etcetera.

Cloud Deployment

In my experience wherever IT is an auxiliary function to other speciality enterprises often lacks technology adoption & skills, security awareness amongst top management, and is the biggest deficit than budgetary constraints. For these enterprises, Cloud deployment is a preferred choice to readily avail relatively more secured deployments within a definitive budget.

Following security measures are offered out of the box in a cloud deployment.

a) Server virtualization (Hypervisors): VMware was the leader in virtualization and laid down NIST guidelines towards Infrastructure as a Service (*Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments*, n.d.). Hypervisors offers OS hardening, Kernel hardening, Layer2 network packet encryption, memory fencing, IPsec for

north/south traffic, network segmentation, Intrusion Detection System (IDS) & Intrusion Prevention Systems (IPS) for hosts/networks (HIDS,NIDS,HIPS,NIPS) and automatic virtual machine isolation etcetera out of the box. It also helps in Asset and Inventory management using Resource Tagging, also helps in secured boot using Hardware Security Module. A shared server hardware resource thus makes it cost effective for both the parties (seller and the consumer) helping to stay abreast to the technological advancements and benefit from security patches at the hypervisor kernels.

b) Software defined networking: SDNs offer VPC (virtual private cloud) segmenting the physical network which can be dynamically configured without waiting for movement/configuration overheads of physical devices. All network functions like routing, vpn etcetera are exposed as NFVs, and thus can be inspected, monitored and audited just like any other application software which is difficult for traditional network hardware elements because of many reasons like lack of standardized apis/logs/statistics across vendors or due to limited compute/memory resources within the device. SDNs enable creation of DMZs to isolate untrusted traffic from the outside world.

c) Virtual Machines (VM): Hypervisors, apart from hardware resource virtualization it also offers several security measures like MPLS/VLAN/Network Port obfuscation/Packet switching, firewall partitioning etcetera. Overall, it gives better control over the guest operating system deployed within a virtual machine. Policy based encryption and access control for the administrators can be applied without the dependency on application developers and are often transparent to the guest o/s. Storage, CPU and memory is also virtualized and hence can be externally bounded, inspected uniformly without dependency on the flavor of guest operating system. When a security incident happens VMs can be moved to a sandbox without interrupting the processing within it and real time forensics can be applied while mitigating against lateral movement of the intruder, giving enormous advantage to the Incidence Response Team. Capacity planning (which is also an attack vector we will see later) can be administered using features like memory ballooning which also helps in avoiding running out of resources due to traffic bursts situations. Dynamic provisioning (ability to destroy or

bring up a virtual machine quickly) helps in several ways from a security perspective towards least exposure of services. Maintaining a "golden copy" of these VM images securely gives a baseline to compare against infected VMs when security events occur.

Software Security: Micro Services (Docker Containers): Containerization is becoming prevalent not only on cloud deployments but on bare metal servers on premise deployments too. Therefore, this deserves a separate topic of its own. Docker containers evolved based on the idea of linux LXDs but much specialized for running applications and ephemeral in nature (*LXD Vs Docker*, 2022). Kubernetes, which essentially helps in automating deployments of many docker containers and interconnecting them, primarily offers network layering transparent to the underlying host (VM or bare metal) networking. Storage virtualization is another key component of containerization. Kubernetes helps manage memory/cpu allocation strategies based on overall clustering of the service(s) instead of per host and applies these policies while spawning containers on hosts based on its available resources in the cluster. This dynamically adapting capability based on capacity helps in mitigating many attack vectors which traditional architectures could not due to its "static" nature or fixed planning mechanics. For example a finalized container image can be centrally controlled, signed and compared later to avoid binary tampering, detect malware injections and most of all if compromised, safeguards against infecting host servers and peer processes. Using sidecar container management, if the attacker succeeds in bringing down the process, it can be respawned without manual intervention and hence mitigates against prolonged downtime. L2 over L3 networking (Young & Ganesan, 2013) enables to form a stretched cluster across geographically separated hosts across multiple datacenters providing a singular view of the network to the applications. Furthermore, with bridged networking (*Docker Networking Overview*, n.d.) an attacker cannot deduce every location of instances of a service bottom up if a physical network gets compromised in one datacenter, keeping the end-user services running, although in reduced capacity. NATing thus avoids bidirectional (top-down or bottom-up) network discovery, restricting lateral movement drastically and automatically containing the breach locally to that

compromised service only. Micro-services also help in stateless processing, meaning user requests can be serviced by any of the multiple instances without needing to have a context of the previous requests made. This is particularly helpful in connection less protocols like http.

Software Security: Service Endpoints (Web Servers):

In today's world of interwebs, web servers are the primary entry point for end users to avail information and services. Therefore, it warrants a separate topic in any security discussion. Now-a-days reverse proxy (*Security Aspects of Using a Reverse Proxy Server*, n.d.) is the first standard line of defense towards securing a web server. Reverse proxy obfuscates the "real" server(s) hosting the website, reducing the possibility of data breaches or DDoS attacks bringing down the whole site by payload inspection, url rewrites, port forwarding, SSL termination, load balancing, sticky sessions, disallowing cross-scripting etcetera.

Web servers typically offer modern authentication schemes such as OAuth (*Web Services Authentication - Business Central*, 2022) that have web service access keys and key managers rotating them periodically.

Web requests are now accessed using RESTful APIs (Gupta & Thomas, 2021) providing stateless processing of each http request independently via any server process. This not only helps in load balancing but helps in identity chaining keeping the server process agnostic to the incoming traffic. From a security point of view this is extremely important because even if one http request succeeds in delivery of a payload and hijacks the server, it is unlikely to take advantage of it on the next request. Thus chaining attacks across multiple http requests becomes harder, replay attacks are also mitigated.

Software Security: Serverless deployments:

Modern systems are adopting serverless computing to scale application programs. Software-as-a-Service hides complexity around resource allocations and as a side effect safeguards against vulnerability scans in case of network breach. Serverless storage like S3 (*Amazon S3 Security*

Features - Amazon Web Services, n.d.) offers out of the box advanced security features to make data breaches or capacity exhaustion even more difficult. IAM based policy management helps mapping "owners" to "services" both from lifecycle management to access management.

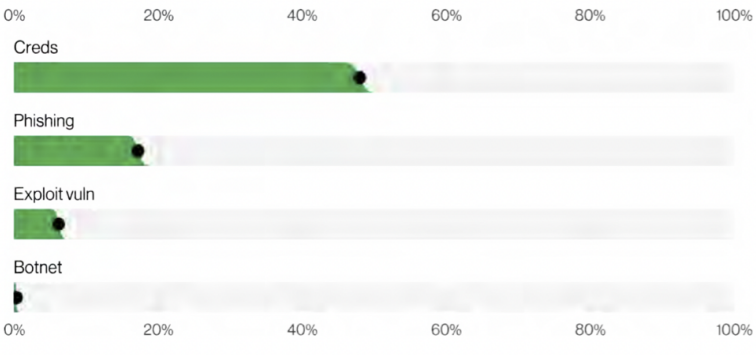
WHY DO WE STILL GET HACKED

So far we have extensively seen how the focus is securing the server(s) alone right from physical security planning/execution to various layers of software security. One primary flaw in this thinking is we treat every incoming user request at par and really doesn't bother distinguishing between "good" or "bad" actors. In other words, the underlying intent of the request is whether malicious or normal is the sole onus of the firewalls/data centers/server(s) to determine and either reject or accept the incoming request respectively. Ofcourse, there are sufficient measures to avoid well known attacks like MTM, replay, DNS spoofing etcetera but there are many kinds of cyber threats.

Statistics and Overview of the Cyber Attacks

According to the DBIR (data breach investigations report) of 2022, 82% breaches are due to human error. (*2022 Verizon DBIR – What Does It Mean?*, 2022)

It's the Human - Figure 09: This finding is most likely the one garnering the greatest attention, clearly calling out that once again people are involved in breaches over 80% of the time. "By people" could mean a breach due to someone clicking on a link in a phishing email, someone reusing a weak password that is compromised, or an IT admin misconfiguring their cloud account and accidentally sharing sensitive data with the entire world. Use this number to help your leadership understand and create a sense of urgency that people, and not just technology, need to be addressed.



There are four key paths leading to your estate: Credentials, Phishing, Exploiting vulnerabilities and Botnets. These four pervade all areas of the DBIR, and no organization is safe without a plan to handle them all.

Figure 5. Select enumerations in non-Error, non-Misuse breaches (n=4,250)

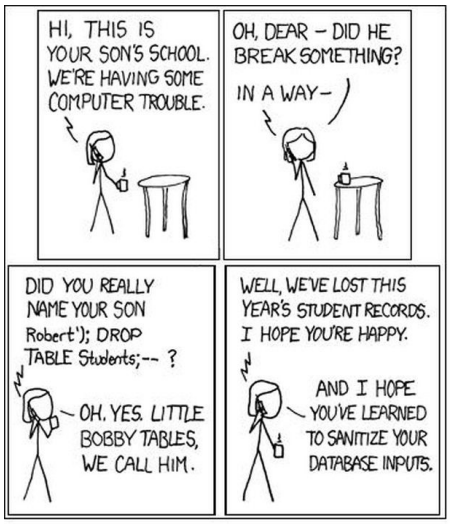
According to this report credential theft and phishing seems to top the chart which is corroborated by another article here but there are many attack vectors as per UpGuard, an integrated attack surface management product company (Sen, n.d.), mainly:

> "Compromised or Weak credentials, Insider Threats, Missing or Poor Encryption, Misconfiguration, Ransomware, Phishing, Vulnerabilities, Brute Force, Distributed Denial of Service, SQL injections, Trojans, Cross-site scripting, Session Hijacking, Man-in-the-middle and third and fourth-party vendors".

Looking at the biggest data breaches until this year (Sen, n.d.), the attacks are quite widespread and there seems to be no commonality on the attack vectors. VMware ESXi hypervisor security blogs published a sleuth of ransomware attacks (Gillis et al., 2022) only this year shows how widespread attack vectors can be.

Common Weakness Attack Vectors

SQL Injection



Looking at the bottom left quadrant in the above meme, it's a classic case where user inputs are used without cleansing for special characters and premature termination of the sql string in conjunction

to using SQL Statement instead of variable binding with SQL PreparedStatements, executed “as is” onto a database (*Common SQL Injection Attacks*, n.d.).

A select statement erroneous code like dbconnection.execute(“SELECT * from Students where user_id = ”” + userinput + ““ “) in particular exposes all sorts of sql injection vulnerabilities mentioned. Penetration testing tools like SQLMap are used to discover such weaknesses but NoSQL using Node.js is fairly recent and on the rise.

Code Injection

This is a more sophisticated but simpler form of Remote Code Execution (*CWE - CWE-94: Improper Control of Generation of Code ('Code Injection') (4.9)*, n.d.). One common use case is wherever the user uploads file(s), for example job sites accepting resumes in pdf or docx format but the program is not doing “input validation” before persisting the file into servers’ local filesystem. Knowing the programming language of the server is written in, a bad actor can guess there will be some system function invocation, for example if server is written in C, following code block can be assumed.

```
fp = fopen("marks.txt", "w");
gets(resume_binary);
fprintf(fp, "%b\n",resume_binary);
fclose(fp);
```

The bold facet code is trying to write the input resume_binary data into the file system without input validation. If this file is an executable, any attempt to read this file using eval or alike will result in executing the arbitrary code instead of opening it into a text processor (GUI or program).

Command Injection

This is very similar to above but is based on the assumption “eval” system function is used with the user input. (*CWE - CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') (4.9)*, n.d.). Extending the above job site example, if a cover letter text input is

attempted to cleanse on the server side using system tools like grep, a program will typically call “eval” function and open for such attacks.

HTML Injection

This is another variant of injection attacks where html tags are utilized. (*HTML Injection Tutorial: Types & Prevention With Examples*, 2022). Often input description fields from the user are open to such attacks where the user is free to write anything & potentially inject html tagged contents that gets executed during “http post” message to the server.

Weak Credentials

Password cracking attacks can be done in many ways viz. dictionary, rainbow tables, NTLM hash generator, domain cached credentials (*Cached and Stored Credentials Technical Overview*, 2016), markov modeling, mask attack (rules and policy based generation), hybrid, combinator attack using hashcat, mdxfind hashcracker, passphrase token attack (Abrams, n.d.), PRINCE and PRINCECEPTION attack, fingerprinting, PACK attacks. Credential cracking distributed system tools like cracklord or hashview and cracking services like gpuhash can be utilized easily to determine md5, SHA-1-512 hashes.

Unfortunately after decades of modern computing, passwords still remains part of MFA (Kanoon, 2022) and thus prone to attacks like SIM-swapping, credential stuffing and account takeovers (*How to Prevent Account Takeover (ATO) | HYPR*, 2022).

Reverse Proxy Attacks

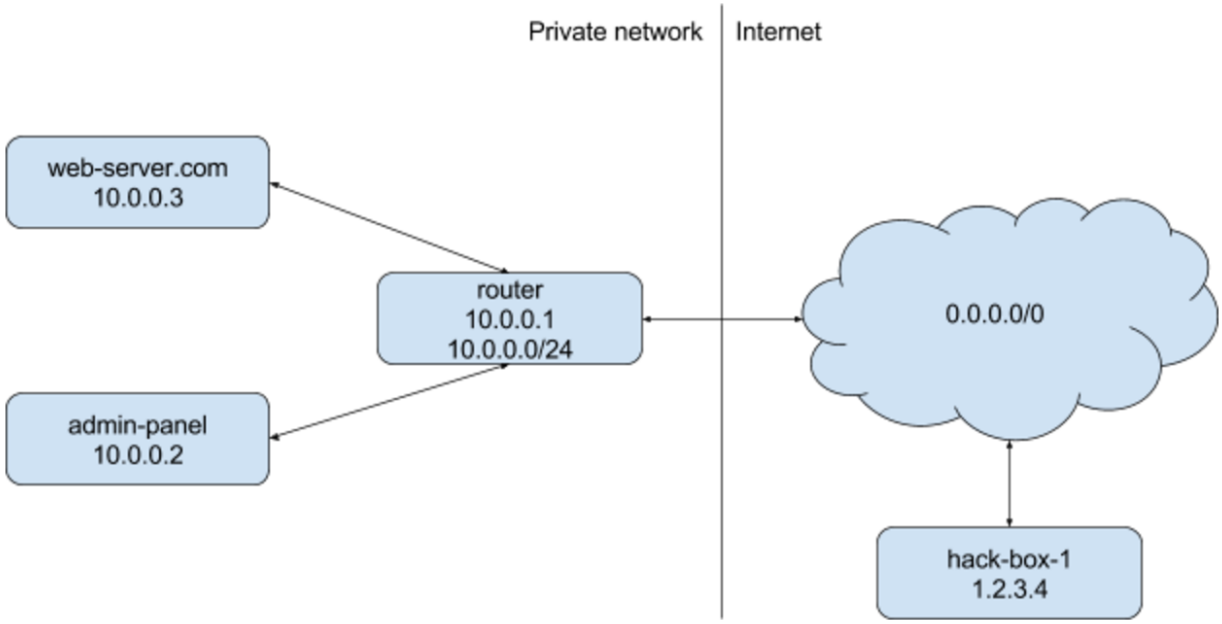
NGINX though offering a lot of protection in safe keeping of the real web servers, it is itself under several attacks (*Top 5 Most Critical NGINX Vulnerabilities Found*, 2022) like SPDY heap buffer overflow, root privilege escalation, integer overflow, controller vulnerability and RCE. There is a whole list of vulnerabilities and advisory until the latest version of NGINX is listed (*Nginx Security Advisories*, n.d.) and continuously patched. Due to the open source nature of it, a complete analysis

(*Possible Arbitrary Code Execution With Null Bytes, PHP, and Old Versions of Nginx » Neal Poole*, 2011) is possible and similar programming errors can be avoided universally.

Cross-Site scripting XSS attack

There are many ways of XSS like polyglot XSS payloads, BeFF (*The Browser Exploitation Framework Project*, n.d.), Blind XSS, DOM based XSS, Advanced NodeJS XSS. (*Cross Site Scripting (XSS)*, n.d.). Essentially, browser plugin download is one such user action opens up this kind of attack where a legitimate site and an unsuspecting user have no clue. This is the reason google doc plugins sends email every time you authorize sharing of your data to third party plugin publishers as a secondary alert.

SSRF (Server Side Request Forgery)



SSRF (*Home*, n.d.) vulnerabilities is nicely shown in the above diagram which is a form of reverse shell attack over the web and a decent explanation can be found here. The core idea is to use "loopback" network adapters to implicitly reach the server as authorized endpoint while piggybacking on the limited access path opened for the user externally. Plain text url rewrites and using http-post makes it simpler than one might think otherwise.

Recent Attack Vectors

Although the common weakness list of attacks and vulnerabilities are long, let's change our focus to recent attacks on state-of-the-art deployments.

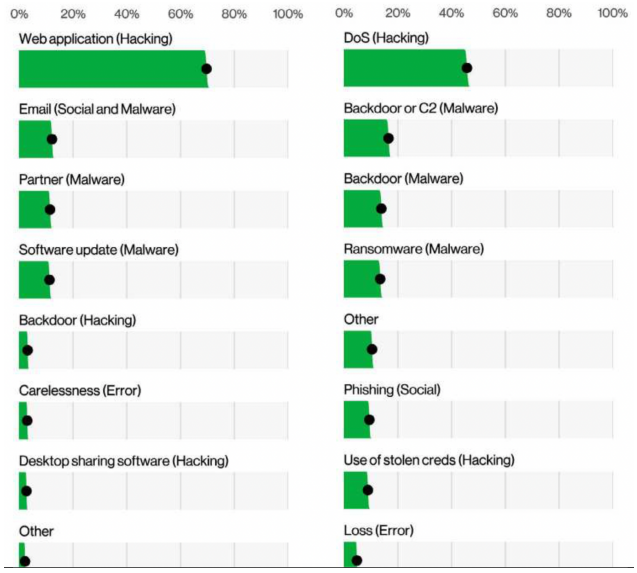
DDoS (Distributed Denial of Service) Attacks

There are several ways and several flavors of DDoS like Zoom Bombing (Nathoo, 2020), (*DHCP Starvation Attack*, 2022), TCP reflection attacks (*Home*, n.d.) and several others like SYN Flood, UDP and ICMP floods, HTTP flood, Ping of Death (Chickowski & Davies, 2020). There are yet others like NTP flood, HTTP fragmentation, Recursive GET Attacks, Synonymous IP attack, Spoofed Session Flood, IP Null Attack, Slowloris etcetera (*35 Types of DDoS Attacks (That Hackers Will Use Against You in 2022)*, n.d.).

Compression Bombs (Jones, 2013), XXE (XML eXternal Entities), Carpet bombing, DNS amplification, Botnets, Distributed Automatic Failover are the few known methods of DDoS that can be effected by just using web requests. URL hijacking (Tuğberk, 2020), search result poisoning (Sharma, 2022), SEO (search engine optimization) poisoning (Toulas, 2022) are more modern subtle forms of DDoS.

Phishing Attacks

Referring back to the DBIR report (*2022 Verizon DBIR – What Does It Mean?*, 2022), we see from the following figure:



that the second most vulnerable method is email phishing compared to other variants like social engineering phishing, but in general phishing is on the rise (Grimes, 2020). Polyglot file infection malware (Toulas, 2022, November 10), IceXLoader via email delivery chain (Toulas, 2022, November 9), ProxyNotShell (Goodin, 2022) are among the latest compromises. According to the latest study, phishing web sites are online for an average 19 hours (*Phishing Sites Online for an Average of 19 Hours*, 2022) as opposed to last year's average uptime of 21 hours.

New Mechanics of Attacks

HTTP Request Smuggling (Vijayan, 2022), Remote Template injection via spear phishing emails in Ukraine attacks (*VBA Macro Remote Template Injection With Unlinking & Self-Deletion*, n.d.), wiper malwares (*CaddyWiper: New Wiper Malware Discovered in Ukraine*, 2022) used by Sandworm in recent Ukraine cyber warfare (*Black Hat USA 2022 | Briefings Schedule*, n.d.), bypassing DKIM/DMARC/SPF email authentication checks intrusion alert based phishing emails (Cash, 2022), infringement phishing attack (Montalbano, 2022), DNS hijacking (*What Is DNS Hijacking and How Does It Work?*, n.d.) are some latest forms of attacks that modern technology is still grappling with.

AppStore and PlayStore vulnerabilities are new forms of endpoint (Toulas, 2022, October 27) attacks where user credentials are compromised using malicious app downloads or trojan infection.

Platform Security based phishing attacks (Meskauskas, 2022) is on rise & compromising millions of user devices.

Infecting Certificate Authority (Goodin, 2022, November 15) and using it as a targeted delivery channel for malwares shows recent advancements of the threat actors.

Generic app misrepresentation (Pearson & Taylor, 2022) is another threat vector that was never seen before. Log4Shell is still in play (Gatlan, 2022) after nearly a year of its discovery (Ducklin, 2021) shows how attackers employ vulnerability scans without being flagged by the most modern IDS/Firewall monitoring systems even with virtualizations.

Following figure (*China-Sponsored Cyberattackers Target Networking Gear to Build Widespread Attack Infrastructure*, 2022) gives us a glimpse of vulnerability types as of today.

Vendor	CVE	Vulnerability Type
Cisco	CVE-2018-0171	Remote Code Execution (RCE)
	CVE-2019-15271	RCE
	CVE-2019-1652	RCE
Citrix	CVE-2019-19781	RCE
DrayTek	CVE-2020-8515	RCE
D-Link	CVE-2019-16920	RCE
Fortinet	CVE-2018-13382	Authentication Bypass
MikroTik	CVE-2018-14847	Authentication Bypass
Netgear	CVE-2017-6862	RCE
Pulse	CVE-2019-11510	Authentication Bypass
	CVE-2021-22893	RCE
QNAP	CVE-2019-7192	Privilege Elevation
	CVE-2019-7193	Remote Inject
	CVE-2019-7194	XML Routing Detour Attack
	CVE-2019-7195	XML Routing Detour Attack
Zyxel	CVE-2020-29583	Authentication Bypass

Out of band attacks (Çıtak, 2019), OOB resource overloading (*Out-Of-Band Resource Load in Google Allows Attacker to Launch a DDoS Attack From Its Servers*, 2017) and DNS tunneling (*Out of Band Exploitation (OOB) CheatSheet*, 2018) shows how network communications are exploited from internet.

Ransomwares and cryptojacking are increasing rapidly and evolving to double extortion and ransomware-as-a-service (*Ransomware Awareness for Holidays and Weekends | CISA*, 2021). Attacks are also being automated for example Drive-by-attack, Machine-in-the-middle attack, IoT based attacks.

As the list of attacks are ever growing, a natural question arises, what are we doing about it.

NOW WHAT ?

With the above partial list of latest attacks we can see a common thread. The incoming user identity is not known in its entirety. In some cases even the remote IP address block is also not known, let alone geo-tagging or device identity or user identity. Looking closely at the above listed historic Vs modern attacks, we can see the latter evolved to a more "top-down" approach as compared to past decade's "bottom-up" approach. We can further see servers are often breached "inside-out" establishing connection to several proxy sites before reaching the command center, making it harder and harder to identify the attackers' ip address or identity. Modern malwares use exponential backoffs, random traffic generation, throttling, dummy windows, and the program code is fitted within a small footprint of bytes (often in a kilobyte) and use chaining, self generation methods to emit dynamic programs.

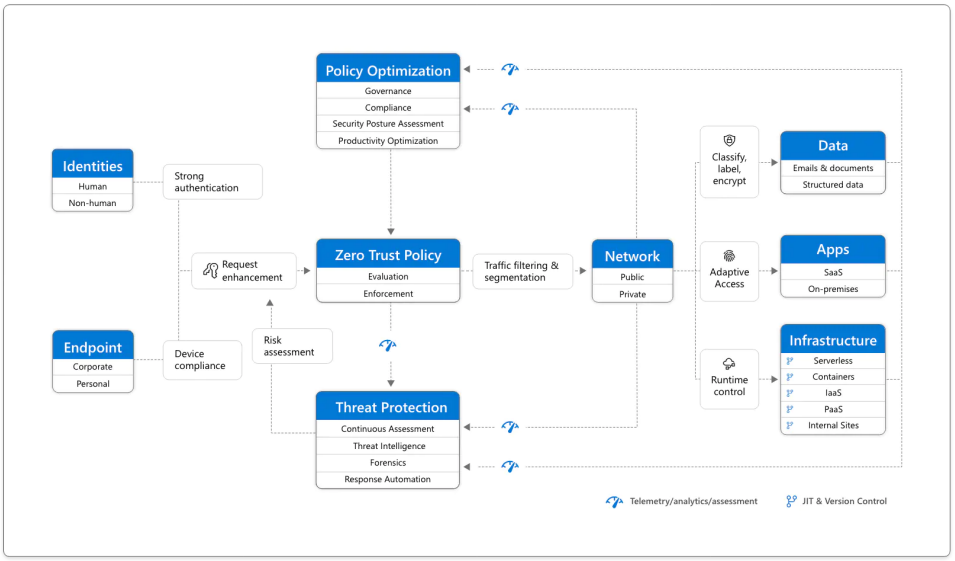
With this ever increasing amount of anonymous users' intrusion, thoroughly identifying the "origin" of the connection and the "originator" themselves is imperative. A simple challenge response server cannot distinguish with certainty between the "good" and the "bad" actors. Edge devices must reveal itself enough to determine who, from where and when it contacted the server and for what (intent), like employee? visitor? user? remote admin? redirected? The server must also know with certainty, are you really who you say you are, collect enough information about you over time, reconcile your next access based on it, personalize authentication around your unique habits and alert

out-of-character behavior, understand the number of devices you use and their identity. In one word, secure the "endpoint" (*Why Perimeter Security Is No Longer Enough*, 2021).

Endpoint Security and Zero Trust:

User operated devices like computers, laptops, mobile phones and tablets all come under edge devices and thus require protection against misuse, compromise, theft, and disposal. Furthermore, with the advent of IoT (internet of things) any object fitted with a microchip i.e., smart devices exhibiting ubiquitous computing warrants physical, hardware & software security, and therefore requires identity revelation, safeguarding and monitoring.

Digital Identity now exists for almost everyone which can be treated as personal identity and must follow highest standards of authentication (*NIST Special Publication 800-63B*, n.d.). Corporates are joining hands towards passwordless authentication (*Apple, Google and Microsoft Commit to Expanded Support for FIDO Standard to Accelerate Availability of Passwordless Sign-Ins*, 2022) instead of incremental improvement of password based security (*Is the Time Complexity to Crack a Hash of a Salted Password Greater Than the Time Complexity to Crack a Hash of an Unsalted Password?*, 2013). On the server side, traditional castle-and-moat deployments are being phased out and corporates are implementing zero trust (*Zero Trust Model - Modern Security Architecture*, n.d.) thus improving on the mutual authentication.



PII Collection and Security:

Personal Identifiable Information collection happens during everyday activity, some for national security (*Examples of PII Collection at DHS*, 2021) and others for benefits (*Understanding PII in Google's Contracts and Policies - Google Ad Manager Help*, n.d.).

Looking at the following list of device details Microsoft gathers for endpoint analytics (*Endpoint Analytics Data Collection - Microsoft Endpoint Manager*, 2022),

- Diagnostic, performance, and usage data tied to a user and/or device
  - **logOnId**
  - **bootId:** The system boot ID
  - **coreBootTimeInMilliseconds:** Time for core boot
  - **totalBootTimeInMilliseconds:** Total boot time
  - **updateTimeInMilliseconds:** Time for OS updates to complete
  - **gpLogonDurationInMilliseconds**: Time for Group policies to process
  - **desktopShownDurationInMilliseconds:** Time for desktop (explorer.exe) to be loaded
  - **desktopUsableDurationInMilliseconds:** Time for desktop (explorer.exe) to be usable
  - **topProcesses:** List of processes loaded during boot with name, with cpu usage stats and app details (Name, publisher, version). For example *{"ProcessName":"svchost","CpuUsage":43,"ProcessFullPath":"C:\\Windows\\System32\\svchost.exe","ProductName":"Microsoft® Windows® Operating System","Publisher":"Microsoft Corporation","ProductVersion":"10.0.18362.1"}*
- Device data not tied to a device or user (if this data is tied to a device or user, Intune treats it as identified data)
  - **ID:** Unique device ID used by Windows Update
  - **localId:** A locally defined unique ID for the device. This ID isn't the human-readable device name. Most likely equal to the value stored at HKLM\Software\Microsoft\SQMClient\MachineId.
  - **aaddeviceid:** Azure Active Directory device ID
  - **orgId:** Unique GUID representing the Microsoft 365 Tenant

We see how the user is decoupled from the device information gathering leading to safer summary statistics storage and processing.

Protection of PII data itself is of huge concern (*PII Data — Protecting Identity Data Across Borders*, 2018), (*12 Ways of Securing PII Data for MSP Companies*, 2021) and any breach can affect millions of users at a time causing a ripple effect of "information security" failures.

BYOD vs COPE:

Corporates' endpoint security policies in an effort to overcome limitations of Bringing Your Own Device (Burgess, 2014) has swiftly moved to Corporate-Owned, Personally Enabled Devices (Ely, 2014) enforcing better control and administration of the corporate network.

User Awareness driven endpoint security

Securing the endpoint device is not enough, security awareness of users are equally important and in conjunction with the knowledge of PII information being collected, users can take creative measures to further resist “social engineering” attacks.

For example, in social sites like twitter/instagram I spell my name phonetically correct but spell differently than my certificate name. Similarly, wherever possible I suppress house numbers and provide only street names of my address, provide nearby zip codes in situations like during a sale pickup in facebook marketplace, have a dedicated email address that is specifically for non-essential purposes like hotel bookings, shopping etcetera., fill out the site name as my middle name while signing up for deals enabling me to track who all are selling my data.

Being aware of attack vectors, I never use password managers for banking sites, use modern payment systems’ latest features if available like generating synthetic vendor specific card numbers or keep my banking habits private, have dedicated credit cards for regular use with lower limits set, enable transaction alerts above a minimum amount I can risk losing, be mindful about “mode” of payment and cards/payment apps used from vendor to vendor, then I make that mode of payment as my preference for that vendor I use regularly.

I am also cautious around what I am browsing on “work” Vs “personal” computer(s)/ device(s), always use “full-disk” encryption, be mindful about clicking on “urls”, plugging in usb devices etc, ask confirmatory questions to arbitrary callers before acknowledging my identity, crosscheck my information with relevant person by initiating a call of my own not through patched/transferred incoming calls. Beware that mobile numbers are modern day “ssn”, deny and be rude instead of being polite & get tagged. Apply least privileges to Apps, ask yourself “why” do you need by contacts/sms/call records, more often than not the app works fine or revoke those privileges from time to time after your work is done. The app is going to ask for it on next usage anyway. Exploit the convenience of biometrics avoiding sharing of “mobile unlock code”, use “wifi barcode scan” feature

of the mobile device to avoid password sharing and keep tabs on the number of devices you have allowed. Secure your wifi router by switching off WPS feature, increase stricter firewall rules like whitelisting devices connected. Block outgoing traffic apart from incoming and selectively open outgoing ports tagging each of them. Commonly used ports (outgoing internet traffic) ruleset is very finite, see the list below:

example home wifi router rules

HTTP and HTTPS -- 80, 443

DNS -- TCP/UDP 53, NTP 119, 123

email -- TCP 25, 110, 143, 465, 587, 993, 995

VPN -- GRE [UDP 500/4500/62515] TCP 1723

DEFAULT setting [Block all outgoing traffic]

Enable Intrusion Detection System and **Disable WPS**.

More home router settings that I typically configure are to turn on DDoS scan, reject ICMP traffic, reduce wifi discovery window from default 30 mins to 3 mins. My mobile device is enabled with remote location tracking and remote wipes features of the manufacturer. I regularly report and block unknown whatsapp messages, always callback when receiving a call from unknown callers "before" divulging any personal information, and look out for the "urgency" level imposed on me during any information gathering action.

DIGITAL MODERNIZATION

Frequency of security breaches and many of them being state sponsored shows Cyberwarfare is real and is being fought (Kessler, 2022) (Lyngaas, 2022) on multiple fronts (*Why Ransomware Attacks Are on the Rise — And What Can Be Done to Stop Them*, 2021).

First and foremost Legislative discussions are happening more frequently than ever (*Managing Cyber Threats Through Effective Governance*, n.d.), (Ramachandran & Vinopal, 2021), (Shields & More, 2022), and cyber laws are becoming specific, clearer and firmer (Ghosh, 2018), (*Senators Draft Bill That Would Require Many Entities to Report Cyber Breaches Within 24 Hours*, 2021), organizations taking a more holistic approach on overall security (*The Mission of the MS-ISAC Is to Improve the Overall Cybersecurity Posture of US State, Local, Tribal, and Territorial (SLTT) Government Organizations Through Coordination, Collaboration, Cooperation, and Increased Communication.*, n.d.). Several books are authored around cyber laws, standards and regulations (KERRIGAN, 2022), (Tari, 2020) in recent times.

Security Standardizations are reactive to the latest threats (*NIST Special Publication (SP) 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations*, n.d.), (*NIST Special Publication (SP) 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, 2010), (Lubell, 2016) and along with standardization of incidence reporting (*CISA Releases Incident and Vulnerability Response Playbooks to Strengthen Cybersecurity for Federal Civilian Agencies*, 2021) Internet Crime Complaint Center (*About IC3*, n.d.) has increased its scope offering a reliable source of cyber crime tracking and cross referencing (https://www.ic3.gov/Media/Y2020/PSA200320).

Security Investigation Reports (Malik, n.d.), (*Threat Intelligence Report 2020*, n.d.), (*FBI IC3 Report for 2021*, n.d.) (*Full Disclosure: Ransomware Exposed*, n.d.) and detailed alerts (*#StopRansomware: Hive Ransomware | CISA*, 2022) are regularly published.

Extensive Research is also happening around machine intelligence specifically to counter cyber attacks (*Ensemble Adversarial Training: Attacks and Defenses – Google Research*, n.d.), (*[1611.01236] Adversarial Machine Learning at Scale*, 2016), tutorials are created to try out various models (Lippe, n.d.). Automated techniques (*Classifying and Tagging PII Fields Residing in BigQuery and Automating Access Control to Them.*, 2022) are developed to safeguard corruption of the ML models itself. Another

noteworthy set of standardization to look forward to is DoD (*Chief Information Officer > Library*, n.d.) showing resolve towards future readiness. For example, committing to definitive timelines enforcing Zero Trust (*DOD ZT Capability Execution Roadmap*, 2022) towards digital modernization. OSINT (Clark, n.d.) tools are being developed to automate pentesting and protect PIIs.

The Software Industrys' response to cyber threats is multifaceted. For example, Google responding to Operation Aurora attack acquired BeyondCorp (Tishbi et al., 2019) leading the industry towards Zero Trust. Similarly, the industry is identifying new ways to summarize information (*73 Ransomware Statistics Vital for Security in 2022*, 2022), aligning Data Governance with Laws and Regulation (Darbellay & Lee, 2022), creating modern firewalls (*Astra Website Protection Features | Firewall | Malware Scanner*, n.d.) with Attacker profiling (geo point/ip address/origin), data scrapers protection, ad & spam bots protection and Threat analytics & ATP doing Real-Time Deep Packet Inspection (*SonicWall Capture Advanced Threat Protection (ATP)*, n.d.). Infrastructure software companies is publishing reports on platform security (*Apple Platform Security*, n.d.), supporting modern security models natively in operating systems kernels upgrading all flavors of linux (Huang, 2022) and approaching end-to-end security holistically (Lubell, 2016). Apart from these important steps, hardware and software products are developed/packaged/hosted & released with a heavy focus on preventing supply chain attacks (Hatti, 2022), (*Content Trust in Docker*, n.d.). Enterprises and software vendors are now aggressively validating open source products, continuously evaluating security aspects of dependent softwares and third party libraries, enforcing static code analysis and vulnerability assessment. Old and new datacenter deployments are finally taking the daunting task of overhauling network infrastructure by adopting IPv6 (Hogg et al., 2021) rapidly, thus reducing the attack surface drastically and eliminating age old possibilities like ARP poisoning (a root cause of several attacks e.g. DDoS & MITM).

CONCLUSION

So far I have walked through the nuts and bolts of (a) Server Architectural security measures (b) Pattern(s) emerging out of the modern attacks bypassing those measures (c) Corrective measures like endpoint security required to safeguard against those breaches. By now readers must recognise "why revelation of some PII (Personal Identifiable Information)" is necessary on the edge device(s) users are using, trading off some privacy over security. Instead of enterprises trying to underplay the fact that PII information is captured by them all the time, I think narration like in this paper is required to "convince" the user to reveal themselves and be "conscious about it". Users must know why he/she has to reveal their behavioral pattern, and whom they are revealing to, and to what extent their PII is given out, not out in the open but to targeted enterprises, entrusting them to keep their PII safe, ensuring that only summary statistics are revealed. This also gives the user an opportunity to devise a plan against "social engineering" being aware of "how" much information is given "where" and "when" (in what pretext). Servers thus whitelisting the "good" endpoints are in a better position not only to identify and reject/investigate "bad" endpoints but capture "suspicious" endpoints, the gray area where legitimate users try for lateral movement and breach other users' privacy. With such an endpoint secured world, with cooperation from a technologically responsible & security aware enduser, robust end-to-end security is possible without compromising "ease of use", and be future ready to unknown ways of attacks, denying grounds to destructive creativity.

References

[1611.01236] Adversarial Machine Learning at Scale. (2016, November 4). arXiv. Retrieved December 5, 2022, from https://arxiv.org/abs/1611.01236

About IC3. (n.d.). Internet Crime Complaint Center. Retrieved December 5, 2022, from https://www.ic3.gov/Home/About

Abrams, R. (n.d.). *Passphrases and the Passphrase Token Attack – SecureIQLab*. SecureIQLab. Retrieved December 1, 2022, from https://secureiqlab.com/passphrases-and-the-passphrase-token-attack/

Amazon S3 Security Features - Amazon Web Services. (n.d.). Amazon AWS. Retrieved November 30, 2022, from https://aws.amazon.com/s3/security/

Apple, Google and Microsoft Commit to Expanded Support for FIDO Standard to Accelerate Availability of Passwordless Sign-Ins. (2022, May 5). FIDO Alliance. Retrieved December 4, 2022, from https://fidoalliance.org/apple-google-and-microsoft-commit-to-expanded-support-for-fido-standard-to-accelerate-availability-of-passwordless-sign-ins/

Apple Platform Security. (n.d.). Apple Support. Retrieved December 5, 2022, from https://support.apple.com/guide/security/welcome/web

Astra Website Protection Features | Firewall | Malware Scanner. (n.d.). Astra Security. Retrieved December 5, 2022, from https://www.getastra.com/website-protection/features

Baadsgaard, J. (2021, June 19). *Cybersecurity Laws & Regulations*. IPOhub. Retrieved November 28, 2022, from https://www.ipohub.org/cybersecurity-laws-regulations/

Bigelow, S. J. (2022, May 18). *How to Design and Build a Data Center*. TechTarget. Retrieved November 28, 2022, from https://www.techtarget.com/searchdatacenter/How-to-design-and-build-a-data-center

Black Hat USA 2022 | Briefings Schedule. (n.d.). Black Hat. Retrieved December 1, 2022, from https://www.blackhat.com/us-22/briefings/schedule/#industroyer2-sandworm39s-cyberwarfare-targets-ukraine39s-power-grid-again-27832

Brown, E. (2016, December 15). *Hardening the Kernel to Protect Against Attackers*. Linux.com. Retrieved November 29, 2022, from https://www.linux.com/news/hardening-kernel-protect-against-attackers/

The Browser Exploitation Framework Project. (n.d.). BeEF - The Browser Exploitation Framework Project. Retrieved December 1, 2022, from https://beefproject.com

Burgess, C. (2014, June 18). *BYOD: Security and Privacy*. RSA Conference. Retrieved December 5, 2022, from https://www.rsaconference.com/library/blog/byod-security-and-privacy

Cached and Stored Credentials Technical Overview. (2016, August 31). Microsoft Learn. Retrieved December 1, 2022, from https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh994565(v=ws.11)

CaddyWiper: New wiper malware discovered in Ukraine. (2022, March 15). WeLiveSecurity. Retrieved December 1, 2022, from https://www.welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine/

Cash, L. (2022, November 17). *Instagram Email Attack: Capture and Share your User Credentials*. Armorblox. Retrieved December 1, 2022, from https://www.armorblox.com/blog/instagram-credential-phishing-email-attack/

Chickowski, E., & Davies, N. (2020, July 8). *The 3 Types of DDoS Attacks Explained*. AT&T Cybersecurity. Retrieved December 1, 2022, from https://cybersecurity.att.com/blogs/security-essentials/types-of-ddos-attacks-explained

Chief Information Officer > Library. (n.d.). DoD CIO. Retrieved December 5, 2022, from https://dodcio.defense.gov/Library/

China-Sponsored Cyberattackers Target Networking Gear to Build Widespread Attack Infrastructure. (2022, June 8). Dark Reading. Retrieved December 1, 2022, from https://www.darkreading.com/threat-intelligence/china-sponsored-cyberattackers-target-networking-gear-to-build-widespread-attack-infrastructure

CISA Releases Incident and Vulnerability Response Playbooks to Strengthen Cybersecurity for Federal Civilian Agencies. (2021, November 16). CISA. Retrieved December 5, 2022, from https://www.cisa.gov/news/2021/11/16/cisa-releases-incident-and-vulnerability-response-playbooks-strengthen

Çıtak, Ö. (2019, December 22). *Out-of-band Attacks [EN] | Omer Citak's Blog | Om3rCitak*. Ömer Çıtak. Retrieved December 5, 2022, from https://omercitak.com/out-of-band-attacks-en/

Clark, R. M. (n.d.). *The Cyber Intelligence Analyst's Cookbook. Volume 1: A primer for ...* EBIN.PUB. Retrieved December 5, 2022, from https://ebin.pub/the-cyber-intelligence-analysts-cookbook-volume-1-a-primer-for-open-source-intelligence-collection-and-applied-research.html

Classifying and tagging PII fields residing in BigQuery and automating access control to them. (2022, September 7). Google Cloud. Retrieved December 5, 2022, from https://cloud.google.com/blog/products/identity-security/how-to-use-google-cloud-to-find-and-protect-pii

Climer, S., & Khan, M. (2020, July 14). *What Are The 7 Layers Of Security? A Cybersecurity Report*. Mindsight. Retrieved October 1, 2022, from https://gomindsight.com/insights/blog/what-are-the-7-layers-of-security/

Common SQL Injection Attacks. (n.d.). Pentest-Tools.com. Retrieved November 30, 2022, from https://pentest-tools.com/blog/sql-injection-attacks

Content trust in Docker. (n.d.). Docker Documentation. Retrieved December 5, 2022, from https://docs.docker.com/engine/security/trust/

Cross Site Scripting (XSS). (n.d.). OWASP Foundation. Retrieved December 1, 2022, from https://owasp.org/www-community/attacks/xss/

CWE - CWE-94: Improper Control of Generation of Code ('Code Injection') (4.9). (n.d.). Common Weakness Enumeration. Retrieved November 30, 2022, from https://cwe.mitre.org/data/definitions/94.html

CWE - CWE-95: Improper Neutralization of Directives in Dynamically Evaluated Code ('Eval Injection') (4.9). (n.d.). Common Weakness Enumeration. Retrieved November 30, 2022, from https://cwe.mitre.org/data/definitions/95.html

Cyber and Network Security | NIST. (n.d.). National Institute of Standards and Technology. Retrieved November 29, 2022, from https://www.nist.gov/itl/cyber-and-network-security

Cybersecurity and Physical Security Convergence. (n.d.). CISA. Retrieved November 28, 2022, from https://www.cisa.gov/cybersecurity-and-physical-security-convergence

Cybersecurity Legislation 2021. (2022, July 1). National Conference of State Legislatures. Retrieved November 28, 2022, from https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2021.aspx

Cybersecurity Unit - Criminal Division. (n.d.). Department of Justice. Retrieved November 28, 2022, from https://www.justice.gov/criminal-ccips/cybersecurity-unit

Darbellay, A., & Lee, J. (2022). *Data Governance in AI, FinTech and LegalTech*. Edward Elgar Publishing Limited.

DHCP Starvation Attack. (2022, July 22). GeeksforGeeks. Retrieved December 1, 2022, from https://www.geeksforgeeks.org/dhcp-starvation-attack/

Docker Networking overview. (n.d.). Docker Documentation. Retrieved November 30, 2022, from https://docs.docker.com/network/

DOD ZT Capability Execution Roadmap. (2022, November 15). DoD CIO. Retrieved December 5, 2022, from https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTExecutionRoadmap.pdf

Ducklin, P. (2021, December 13). *Log4Shell explained – how it works, why you need to know, and how to fix it*. Naked Security. Retrieved December 1, 2022, from https://nakedsecurity.sophos.com/2021/12/13/log4shell-explained-how-it-works-why-you-need-to-know-and-how-to-fix-it/

ECS data center have best-in-class physical security standards – All about Tier 4 Data center. (n.d.). ECS Biztech. Retrieved November 28, 2022, from https://www.ecsbiztech.com/ecs-data-center-have-best-in-class-physical-security/

Ely, A. (2014, September 3). *Enterprise Mobility: COPE vs. BYOD*. SecurityWeek. Retrieved December 5, 2022, from https://www.securityweek.com/enterprise-mobility-cope-vs-byod

Endpoint analytics data collection - Microsoft Endpoint Manager. (2022, November 18). Microsoft Learn. Retrieved December 5, 2022, from https://learn.microsoft.com/en-us/mem/analytics/data-collection

Ensemble Adversarial Training: Attacks and Defenses – Google Research. (n.d.). Google Research. Retrieved December 5, 2022, from https://research.google/pubs/pub46638/

European Parliament and of the Council of 6 July 2016. (n.d.). YouTube. Retrieved November 28, 2022, from https://eur-lex.europa.eu/eli/dir/2016/1148

Examples of PII Collection at DHS. (2021, January 4). Homeland Security. Retrieved December 4, 2022, from https://www.dhs.gov/privacy-training/examples-pii-collection-dhs

FBI IC3 report for 2021. (n.d.). Internet Crime Complaint Center. Retrieved December 5, 2022, from https://www.ic3.gov/Home/AnnualReports

44 USC CHAPTER 35, SUBCHAPTER II: INFORMATION SECURITY. (n.d.). U.S. Code. Retrieved November 28, 2022, from https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title44-chapter35-subchapter2&edition=prelim

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (2018, April 16). NIST Technical Series Publications. Retrieved November 29, 2022, from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Full Disclosure: Ransomware Exposed. (n.d.). Knowledge Hub Media. Retrieved December 5, 2022, from https://knowledgehubmedia.com/full-disclosure-ransomware-exposed/

Gatlan, S. (2022, November 16). *US govt: Iranian hackers breached federal agency using Log4Shell exploit*. Bleeping Computer. Retrieved December 1, 2022, from https://www.bleepingcomputer.com/news/security/us-govt-iranian-hackers-breached-federal-agency-using-log4shell-exploit/

Ghosh, D. (2018, July 11). *What You Need to Know About California's New Data Privacy Law*. Harvard Business Review. Retrieved December 5, 2022, from https://hbr.org/2018/07/what-you-need-to-know-about-californias-new-data-privacy-law

Gillis, T., Holzworth, M., Vigna, G., Boyarchuk, O., Ortolani, S., & Haruyama, T. (2022, September 28). *ESXi-Targeting Ransomware: The Threats That Are After Your Virtual Machines (Part 1)*. VMware Blogs. Retrieved November 30, 2022, from https://blogs.vmware.com/security/2022/09/esxi-targeting-ransomware-the-threats-that-are-after-your-virtual-machines-part-1.html

Goodin, D. (2022, November 8). *Patches for 6 0-days under active exploit are now available from Microsoft*. Ars Technica. Retrieved December 1, 2022, from https://arstechnica.com/information-technology/2022/11/patches-for-6-zero-days-under-active-exploit-are-now-available-from-microsoft/

Goodin, D. (2022, November 15). *State-sponsored hackers in China compromise certificate authority*. Ars Technica. Retrieved December 1, 2022, from https://arstechnica.com/information-technology/2022/11/state-sponsored-hackers-in-china-compromise-certificate-authority/

Grimes, R. (2020, March 31). *70% to 90% of All Malicious Breaches are Due to Social Engineering and Phishing Attacks*. KnowBe4 Blog. Retrieved December 5, 2022, from https://blog.knowbe4.com/70-to-90-of-all-malicious-breaches-are-due-to-social-engineering-and-phishing-attacks

Gupta, L., & Thomas, R. (2021, September 30). *Statelessness in REST APIs*. REST. Retrieved November 30, 2022, from https://restfulapi.net/statelessness/

Hatti, A. (2022, July 6). *Jenkins 0 days & Your Supply Chain Security*. PureID. Retrieved December 5, 2022, from https://www.pureid.io/jenkins-0-days-your-supply-chain-security/

Hogg, S., Rose, B., Makaram, N., & Horley, E. (2021, September 1). *IPv6 Enhances Zero-Trust Network Architectures*. Infoblox Blog. Retrieved December 5, 2022, from https://blogs.infoblox.com/ipv6-coe/ipv6-enhances-zero-trust-network-architectures/

Home. (n.d.). Server Side Request Forgery. Retrieved December 1, 2022, from https://www.hackerone.com/application-security/how-server-side-request-forgery-ssrf

Home. (n.d.). YouTube. Retrieved December 1, 2022, from https://cyware.com/news/the-state-of-tcp-reflection-attacks-2cadd82d/

How to Prevent Account Takeover (ATO) | HYPR. (2022, February 28). HYPR Blog. Retrieved December 4, 2022, from https://blog.hypr.com/how-to-prevent-account-takeover

HTML Injection Tutorial: Types & Prevention with Examples. (2022, October 25). Software Testing Help. Retrieved November 30, 2022, from https://www.softwaretestinghelp.com/html-injection-tutorial/

Huang, F. (2022, May 17). *A Zero Trust, Open Source, Cloud Native Security Model*. SUSE. Retrieved December 5, 2022, from https://www.suse.com/c/a-zero-trust-open-source-cloud-native-security-model/

Is the time complexity to crack a hash of a salted password greater than the time complexity to crack a hash of an unsalted password? (2013, December 30). Stack Overflow. Retrieved December 5, 2022, from https://stackoverflow.com/questions/20846643/is-the-time-complexity-to-crack-a-hash-of-a-salted-password-greater-than-the-tim

Is Your Server Secure Enough? (2017, February 10). RTS Labs. Retrieved October 1, 2022, from https://rtslabs.com/is-your-server-secure-enough/

IT Asset Management: NIST Publishes Cybersecurity Practice Guide, Special Publication 1800-5 | NIST. (2018, September 7). National Institute of Standards and Technology. Retrieved November 28, 2022, from https://www.nist.gov/news-events/news/2018/09/it-asset-management-nist-publishes-cybersecurity-practice-guide-special

Jones, G. (2013, August 20). *Vulnerabilities That Just Won't Die - Compression Bombs*. Cyberis. Retrieved December 1, 2022, from https://www.cyberis.com/article/vulnerabilities-just-wont-die-compression-bombs

Kanoon, A. (2022, September 2). *Multi-Factor Authentication (MFA) Is Not Enough*. Banyan Security. Retrieved December 4, 2022, from https://www.banyansecurity.io/blog/multi-factor-authentication-mfa-is-not-enough/

KERRIGAN, C. (2022). *Artificial Intelligence: Law and Regulation. (2022)*. Edward Elgar Publishing. http://dx.doi.org/10.4337/9781800371729

Kessler, G. (2022, October 26). *Analysis | The strange twists and turns of an alleged election conspiracy*. The Washington Post. Retrieved December 5, 2022, from

https://www.washingtonpost.com/politics/2022/10/26/strange-twists-turns-an-alleged-election-conspiracy/

Lippe, P. (n.d.). *Adversarial_Attacks.ipynb - Colaboratory*. Google Colab. Retrieved December 5, 2022, from https://colab.research.google.com/github/phlippe/uvadlc_notebooks/blob/master/docs/tutorial_notebooks/tutorial10/Adversarial_Attacks.ipynb

Lubell, J. (2016, August 1). *Integrating Top-down and Bottom-up Cybersecurity Guidance using XML*. National Institute of Standards and Technology. Retrieved December 5, 2022, from https://www.nist.gov/publications/integrating-top-down-and-bottom-cybersecurity-guidance-using-xml

LXD vs Docker. (2022, March 31). Ubuntu. Retrieved November 30, 2022, from https://ubuntu.com/blog/lxd-vs-docker

Lyngaas, S. (2022, October 5). *Russian hackers knock US state government websites offline*. CNN. Retrieved December 5, 2022, from https://www.cnn.com/2022/10/05/politics/russian-hackers-state-government-websites/index.html

Malik, J. (n.d.). *WHITEPAPER: Using Threat Intelligence to Build Data‑Driven Defense*. KnowBe4. Retrieved December 5, 2022, from https://www.knowbe4.com/hubfs/UsingThreatIntelligencetoBuildDataDrivenDefense.pdf

Managing Cyber Threats through Effective Governance. (n.d.). CIS Center for Internet Security. Retrieved December 5, 2022, from https://www.cisecurity.org/insights/white-papers/managing-cyber-threats-through-effective-governance

Meskauskas, T. (2022, July 8). *Apple Platform Security POP-UP Scam (Mac) - Removal steps, and macOS cleanup (updated)*. PCRisk.com. Retrieved December 5, 2022, from https://www.pcrisk.com/removal-guides/19829-apple-platform-security-pop-up-scam-mac

The mission of the MS-ISAC is to improve the overall cybersecurity posture of US State, Local, Tribal, and Territorial (SLTT) government organizations through coordination, collaboration, cooperation, and increased communication. (n.d.). CIS Center for Internet Security. Retrieved December 5, 2022, from https://www.cisecurity.org/ms-isac

Montalbano, E. (2022, October 27). *Cyberattackers Target Instagram Users With Threats of Copyright Infringement*. Dark Reading. Retrieved December 1, 2022, from https://www.darkreading.com/application-security/cyberttackers-target-instagram-users-threats-copyright-infringement

Nathoo, Z. (2020, April 4). *'Zoom-bombing' attacks on video conferencing platform leave victims shaken*. CBC. Retrieved December 1, 2022, from https://www.cbc.ca/news/science/zoombombing-fbi-warning-1.5519024

nginx security advisories. (n.d.). Nginx.org. Retrieved December 1, 2022, from https://nginx.org/en/security_advisories.html

NIST Special Publication 800-63B. (n.d.). NIST Pages. Retrieved December 4, 2022, from https://pages.nist.gov/800-63-3/sp800-63b.html

NIST Special Publication (SP) 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). (2010, April 6). NIST Computer Security Resource Center. Retrieved December 5, 2022, from https://csrc.nist.gov/publications/detail/sp/800-122/final

NIST Special Publication (SP) 800-162, Guide to Attribute Based Access Control (ABAC) Definition and Considerations. (n.d.). NIST Computer Security Resource Center. Retrieved December 5, 2022, from https://csrc.nist.gov/publications/detail/sp/800-162/final

Obeng, S. (2016, April 28). *Hardware Security Thorough Supply Chain Assurance | NIST*. National Institute of Standards and Technology. Retrieved November 28, 2022, from https://www.nist.gov/publications/hardware-security-thorough-supply-chain-assurance

Out of Band Exploitation (OOB) CheatSheet. (2018, August 30). NotSoSecure. Retrieved December 5, 2022, from https://notsosecure.com/out-band-exploitation-oob-cheatsheet

Out-of-band resource load in Google allows attacker to launch a DDoS attack from its servers. (2017, February 24). Security Affairs. Retrieved December 5, 2022, from https://securityaffairs.co/wordpress/56618/hacking/google-ddos.html

Pearson, J., & Taylor, M. (2022, November 16). *EXCLUSIVE Russian software disguised as American finds its way into U.S. Army, CDC apps*. Reuters. Retrieved December 1, 2022, from https://www.reuters.com/technology/exclusive-russian-software-disguised-american-finds-its-way-into-us-army-cdc-2022-11-14/

Phishing sites online for an average of 19 hours. (2022, April 15). Cyber Threat Intelligence. Retrieved December 1, 2022, from https://cyberthreatintelligence.com/analytics/phishing-sites-online-for-an-average-of-19-hours/

phoenixNAP. (2019, April 20). *21 Server Security Tips & Best Practices To Secure Your Server Quickly*. phoenixNAP. Retrieved October 1, 2022, from https://phoenixnap.com/kb/server-security-tips

PII Data — Protecting Identity Data Across Borders. (2018, August 21). Trulioo. Retrieved December 5, 2022, from https://www.trulioo.com/blog/compliance/pii-data

Possible Arbitrary Code Execution with Null Bytes, PHP, and Old Versions of nginx » Neal Poole. (2011, August 2). Neal Poole. Retrieved December 1, 2022, from https://nealpoole.com/blog/2011/08/possible-arbitrary-code-execution-with-null-bytes-php-and-old-versions-of-nginx/

Ramachandran, V., & Vinopal, C. (2021, June 17). *WATCH: Local, state leaders testify on emerging cybersecurity threats*. PBS. Retrieved December 5, 2022, from https://www.pbs.org/newshour/politics/watch-live-local-state-leaders-testify-on-emerging-cyber security-threats

Ransomware Awareness for Holidays and Weekends | CISA. (2021, August 31). US-CERT. Retrieved December 5, 2022, from https://www.cisa.gov/uscert/ncas/alerts/aa21-243a

Ridgeback. (2018, December 5). *Annual IT Security Spend Has Grown From $3bn to $120bn Since 2003, And We're Still Not Secure*. YouTube. Retrieved October 1, 2022, from http://ridgebacknet.com/wp-content/uploads/2022/01/Ridgeback-eBook-1.pdf

Secure Boot overview. (2021, February 21). Dell. Retrieved November 29, 2022, from https://www.dell.com/support/kbdoc/en-us/000145423/secure-boot-overview

Security Aspects of Using a Reverse Proxy Server. (n.d.). Security Aspects of Using a Reverse Proxy Server. Retrieved November 30, 2022, from https://docs.microfocus.com/UCMDB/11.0/ucmdb-docs/docs/eng/doc_lib/Content/hardening/hard_rproxy_security.htm

Sen, K. (n.d.). *The 68 Biggest Data Breaches (Updated for November 2022)*. UpGuard. Retrieved November 30, 2022, from https://www.upguard.com/blog/biggest-data-breaches

Sen, K. (n.d.). *16 Common Attack Vectors in 2022*. UpGuard. Retrieved November 30, 2022, from https://www.upguard.com/blog/attack-vector#toc-3

Senators draft bill that would require many entities to report cyber breaches within 24 hours. (2021, June 17). CNN. Retrieved December 5, 2022, from https://www.cnn.com/2021/06/16/politics/bill-report-cyber-breach-24-hours/index.html

73 Ransomware Statistics Vital for Security in 2022. (2022, March 5). Panda Security. Retrieved December 5, 2022, from https://www.pandasecurity.com/en/mediacenter/security/ransomware-statistics/

Sharma, A. (2022, November 18). *Google Search results poisoned with torrent sites via Data Studio*. Bleeping Computer. Retrieved December 1, 2022, from https://www.bleepingcomputer.com/news/security/google-search-results-poisoned-with-torrent-sites-via-data-studio/

Shields, M., & More, R. (2022, December 2). *Swiss seek mandatory reporting of cyberattacks on key infrastructure*. 1450 AM 99.7 FM WHTC. Retrieved December 5, 2022, from https://whtc.com/2022/12/02/swiss-seek-mandatory-reporting-of-cyberattacks-on-key-infrastructure/

SonicWall Capture Advanced Threat Protection (ATP). (n.d.). SonicWall. Retrieved December 5, 2022, from https://www.sonicwall.com/products/capture-advanced-threat-protection/

#StopRansomware: Hive Ransomware | CISA. (2022, November 17). US-CERT. Retrieved December 5, 2022, from https://www.cisa.gov/uscert/ncas/alerts/aa22-321a

Tari, S. (2020). *Cybersecurity Law, Standards and Regulations* (2nd Edition ed.). Rothstein Publishing.

35 Types of DDoS Attacks (That Hackers Will Use Against You in 2022). (n.d.). JavaPipe. Retrieved December 1, 2022, from https://javapipe.com/blog/ddos-types/

Threat Intelligence Report 2020. (n.d.). Nokia. Retrieved December 5, 2022, from https://www.nokia.com/networks/portfolio/cyber-security/threat-intelligence-report-2020/

Tishbi, L., Goel, P., & McWilliams, J. (2019, June 27). *Google Online Security Blog: How Google adopted BeyondCorp*. Google Security Blog. Retrieved December 5, 2022, from https://security.googleblog.com/2019/06/how-google-adopted-beyondcorp.html

Top 5 Most Critical NGINX Vulnerabilities Found. (2022, February 4). Astra Security. Retrieved December 1, 2022, from https://www.getastra.com/blog/911/top-5-most-critical-nginx-vulnerabilities-found/

Toulas, B. (2022, October 27). *Drinik Android malware now targets users of 18 Indian banks*. Bleeping Computer. Retrieved December 1, 2022, from

https://www.bleepingcomputer.com/news/security/drinik-android-malware-now-targets-users-of-18-indian-banks/

Toulas, B. (2022, November 9). *15,000 sites hacked for massive Google SEO poisoning campaign*. Bleeping Computer. Retrieved December 1, 2022, from https://www.bleepingcomputer.com/news/security/15-000-sites-hacked-for-massive-google-seo-poisoning-campaign/

Toulas, B. (2022, November 9). *New StrelaStealer malware steals your Outlook, Thunderbird accounts*. Bleeping Computer. Retrieved December 1, 2022, from https://www.bleepingcomputer.com/news/security/new-strelastealer-malware-steals-your-outlook-thunderbird-accounts/

Toulas, B. (2022, November 10). *Phishing drops IceXLoader malware on thousands of home, corporate devices*. Bleeping Computer. Retrieved December 1, 2022, from https://www.bleepingcomputer.com/news/security/phishing-drops-icexloader-malware-on-thousands-of-home-corporate-devices/

Tracy, M., Jansen, W., Scarfone, K., & Butterfield, J. (n.d.). *NIST SP 800-123, Guide to General Server Security*. NIST Technical Series Publications. Retrieved November 29, 2022, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf

Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments. (n.d.). NIST Technical Series Publications. Retrieved November 29, 2022, from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-19.pdf

Tuğberk, K. (2020, August 14). *URL Hijacking: Definition and Avoiding Methods*. Holistic SEO. Retrieved December 1, 2022, from https://www.holisticseo.digital/technical-seo/url-hijacking/

12 Ways of Securing PII Data for MSP Companies. (2021, April 5). N-able. Retrieved December 5, 2022, from https://www.n-able.com/blog/securing-pii-data-12-ways

2022 Data Breach Investigations Report. (n.d.). Verizon. Retrieved December 1, 2022, from https://www.verizon.com/business/resources/reports/dbir/

2022 Verizon DBIR – What Does it Mean? (2022, June 9). SANS Institute. Retrieved November 30, 2022, from https://www.sans.org/blog/2022-verizon-dbir-what-does-it-mean/

Understanding PII in Google's contracts and policies - Google Ad Manager Help. (n.d.). Google Support. Retrieved December 4, 2022, from https://support.google.com/admanager/answer/7686480?hl=en

US and EU Data Localization and Data Transfer Restriction Laws. (2021, August 10). National Law Review. Retrieved November 28, 2022, from https://www.natlawreview.com/article/data-localization-and-data-transfer-restrictions

VBA Macro Remote Template Injection With Unlinking & Self-Deletion. (n.d.). John Woodman's Security Blog. Retrieved December 1, 2022, from https://john-woodman.com/research/vba-macro-remote-template-injection/

Vijayan, J. (2022, August 10). *New HTTP Request Smuggling Attacks Target Web Browsers*. Dark Reading. Retrieved December 1, 2022, from https://www.darkreading.com/application-security/researcher-at-black-hat-describes-new-htpp-request-smuggling-attack

Web Services Authentication - Business Central. (2022, April 27). Microsoft Learn. Retrieved November 30, 2022, from https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/webservices/web-services-authentication

What is DNS Hijacking and How Does it Work? (n.d.). SentinelOne. Retrieved December 5, 2022, from https://www.sentinelone.com/cybersecurity-101/dns-hijacking/

What is Systems Hardening? (n.d.). BeyondTrust. Retrieved November 29, 2022, from https://www.beyondtrust.com/resources/glossary/systems-hardening

Why Perimeter Security is No Longer Enough. (2021, June 16). Cyolo. Retrieved December 4, 2022, from https://cyolo.io/blog/why-perimeter-security-is-no-longer-enough/

Why ransomware attacks are on the rise — and what can be done to stop them. (2021, July 8). PBS. Retrieved December 4, 2022, from https://www.pbs.org/newshour/nation/why-ransomware-attacks-are-on-the-rise-and-what-can-be-done-to-stop-them

Young, J., & Ganesan, M. (2013, July 9). *L2 Bridging Across an L3 Network Configuration Example*. Cisco. Retrieved November 30, 2022, from https://www.cisco.com/c/en/us/support/docs/ip/layer-two-tunnel-protocol-l2tp/116266-configure-l2-00.html

Zero Trust Model - Modern Security Architecture. (n.d.). Microsoft. Retrieved December 4, 2022, from https://www.microsoft.com/en-us/security/business/zero-trust