Clouded views: navigating the complex landscape of digital security - data protection in today's electronic world

A paper based on a presentation to the Institute in Sydney on 22 October 2024 by

Thomas Hamer

This paper describes the current online electronic/digital environment where the protection and management of our electronic intellectual capital are being undermined and have become paramount. This multifaceted aspects of digital security, exploring how conceptual thinking about the electronic systems must adapt to the modern supply chains realties and logistical systems are explained.

Key words: electronic; digital; digital infrastructure; cloud services; supply chain; intellectual property; encryption.

In today's rapidly evolving electronic world, we find ourselves at a critical juncture where the protection and management of our electronic intellectual capital have become paramount. This article delves into the multi-faceted aspects of digital security, exploring how our conceptual thinking about these systems must adapt to the realities of modern supply chains and logistical systems.

While it may be interesting to think about specific individual parts of how we interact with these systems, the entire supply chain needs to be examined in terms of build, run, and maintaining those systems.

Long gone are the days when the internet was merely a place for browsing web pages and sending emails. Today, we not only use but heavily rely on the internet for crucial systems that underpin our daily lives. Connected vehicles, emergency services systems, traffic signals, navigation, banking, and retail are just a few examples of how deeply the internet has become ingrained in our society.

The consequences of internet disruptions have escalated from minor inconveniences to potentially life-altering events. A part of the web going offline can now prevent you from paying bills, navigating to your destination, or even accessing critical emergency services. This increased reliance underscores the need for robust, resilient systems and comprehensive security measures.

Understanding cloud services

Cloud Services is often misunderstood and peoples imagination tells them that the cloud is something up in the sky, but, can be easily explained as a data centre service that you can hire from a third party company to run your own workloads, and, make use of higher order abstractions of information technology (IT) that you do not have to build out yourself, like Machine Learning, or Data Warehousing solutions. As these systems get better and more efficient, companies are abstracting some of their services to make them easier to use, and more flexible. For instance, some cloud services now offer function-as-a-service (FaaS) models, where users can rent a function that runs discrete computational tasks on demand, paying only for the execution time. These abstractions provide innovative ways to utilise cloud services at competitive prices, provided the application is well-designed.

Complexity of modern systems

As we continue to build newer solutions and create better abstractions of the previous generations of systems, the complexity of those systems becomes more significant. This means, that the people we entrust to build run and maintain those systems are a highly important consideration in terms of their skill, knowledge, and trustworthiness become critical factors in ensuring the security and reliability of our digital infrastructure. It is important that we fully consider the supply chain of how we deal with every step of our important infrastructure solutions. With the use of some of these building blocks, it is not necessary that everyone need to create every block of the application, but as we outsource some of the building blocks we must be careful about to whom those building blocks are sourced from (https://xkcd.com/2347/).

Real-world examples highlight the potential dangers. There have been instances where developers have contributed to crucial security modules of important structural software, building up trust, only to later attempt to insert backdoors. The recent case of the XZ Utils backdoor serves as a stark reminder of the vulnerabilities that can arise in the software supply chain (https://en.wikipedia.org/wiki/XZ_Utils_backdoor).

While supply chain considerations are important, it is also important to be thinking about what you keep inside your systems. Should an attacker breach your systems, what could they possibly get a hold of? Intel-

lectual property of the company is a big consideration, however, what about the users?

If user credentials are poorly managed, and their passwords can be extracted, it is possible that those users with other accounts elsewhere could now also be breached. Did the company keep a copy of important secret information, where they did not need to? Drivers licence numbers, tax file numbers, etc that could now be public following a breach.

Poor management of user credentials, particularly passwords can lead to cascading security breaches across multiple platforms. Moreover, companies must carefully consider whether they truly need to retain certain types of sensitive information, such as driver's license numbers or tax file numbers, which could have severe consequences if exposed in a breach.

Data collection and government access

Companies nowadays need to carefully think about the types of data that they choose to collect, and store not just in terms of how that might look if that company was to have their data exposed, but also in terms of whether or not any government agencies might come knocking and asking for that data to be shared. An example of this type of intrusion can be illustrated with nearly all users of Android or Apple mobile devices have their location data constantly streamed back to the Google or Apple servers. Even if you were to never save anyone's contact information, or send any communication via that device, it could easily be implied that you are in contact with another party just through correlating location time and dates where you might have consistently been in the same location as another person on a consistent basis (https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html). The pervasive nature of data collection is exemplified by the constant streaming of location data from Android and Apple mobile devices back to their respective servers.

Understanding encryption and its limitations

While it is not necessary to have a concrete understanding of encryption, it is helpful to have a mental model of how it works and its limitations. We covered what a key exchange is, and the concept of how a cypher works. One of those limitations is things don't stay encrypted when they are used on the device. For the applications to use the data it must be decrypted once it arrives in the target device. Once the data is decrypted on the device, depending on the setup, the device can then potentially have full access to the data. Although it may be possible that just the application has that access, where it comes to applications like Encrypted Messaging applications, as those types of privacy focused applications do not store their chats in plain text in storage. The phone could screen capture whatever is on the display, also circumventing the encryption. Encryption of data in transit is as important as the encryption of data at rest in your device.

Personal threat profiles

If Google or another errant application has some control of system settings, a screen recording could capture whatever is on the display, however, it is also important to consider your personal threat profile. How important are you? Does anyone care about the memes you send to your friends? Are you a road worker sending funny pictures to your colleagues, or are you the CEO of a large multinational company with government contracts? Understanding your threat profile helps in prioritising security measures and allocating resources effectively. While everyone should maintain a baseline level of security, individuals in high-risk positions may need to implement additional layers of protection and be more vigilant about their digital footprint.

Best practices for digital security

Regardless of your threat profile, there are several best practices that everyone should follow to enhance their digital security:

- ***Regular patching and updates***: Install updates from vendors promptly to address known vulnerabilities.
- ***Frequent backups***: Regularly back up your data to protect against data loss due to hardware failure or ransomware attacks.
- ***Multi-factor authentication (MFA)***: Use MFA wherever available to add an extra layer of security beyond passwords.
- ***Email vigilance***: Be cautious about opening emails and attachments, especially from unknown sources. Verify sender addresses and domain names carefully. Be very careful what emails and attachments you open, and verify the sender address and domain name tom@outlook.com is a real email from a Microsoft outlook, domain tom@outlook.123.vip is not.
- ***Physical security***: Ensure your devices are physically secure to prevent unauthorised access via USB or ethernet ports.

Business security considerations

If you are running a business, it is important to monitor your software and hardware activity. You should be aware of what your systems baseline for activity is, and be able to detect deviations from normal. For businesses, security considerations extend beyond individual best practices. It is crucial to implement comprehensive monitoring of software and hardware activity. Establishing a baseline for normal system activity allows for the detection of anomalies that could indicate a security breach. Implementing a robust security information and event management (SIEM) system can help businesses collect, analyse, and correlate security events from various sources across their network. This proactive approach enables faster detection and response to potential security incidents.

Reality of bulk data collection

Your data is being bulk collected. Governments both domestic and foreign, and private companies are bulk collecting traffic on the internet with differing levels of completeness and complexity. Seemingly, the majority of that data is just noise, however it does provide a catalogue of communications between network users where they can peer into the past and see who has said something to another network user. It also appears to be the case that that encrypted data can be decrypted by those government organisations should the need be serious enough. The common man still seems to have little to fear in this regard. This however does not make it a point to be missed. As the saying goes 'if you think you have nothing to hide', just go ahead and read me out your credit card details. None of my business right? While the average person may have little to fear from this level of surveillance, it raises significant privacy concerns and highlights the importance of being mindful about our digital footprint.

DevSecOps: integrating security into development

The DevSecOps (Development Security Operations) approach integrates security practices into the software development lifecycle from the outset. This methodology aims to make everyone accountable for security, with the objective of implementing security decisions and actions at the same scale and speed as development and operations decisions and actions. Key principles of DevSecOps include:

- Shifting security left (earlier in the development process), security is not an afterthought, rather built right into the applications foundations from the start.
- Automating security checks and tests where well known issues are likely to appear and check for them prior to allowing the release of the software package.
- Fostering collaboration between development, operations, and security teams.
- Continuous monitoring and rapid response to security issues.

By embedding security into every phase of the software development process, organisations can reduce vulnerabilities and improve their overall security posture.

Impact on defence and national security

Given the complexity, risk, and ever changing cat-and-mouse-game of information technology, our government and defence community can ill afford to fall behind, or worse, ignore the cyber race that is now on. Australia is well positioned, and has the talent within our boarders to both upskill our people, and, to lead the way in cyber offensive and defensive operations. Each war that took place throughout history built on the skills and tactics before it. WWII resembled but built on WWI and so on with each conflict following it, Korea, Viet-Nam, Afghanistan 1 and 2, and now into Ukraine. We see stark differences in the tooling being used generation to generation. Now that networks are so ubiquitous and our reliance on them is so high, it was only ever a matter of time until this became the latest battlefront. Although not waged with kinetic forces, rather with programs and software, warfare none the less.

Conclusion

As we navigate the complex landscape of digital security, it's clear that a multifaceted approach is necessary. From understanding the nuances of cloud services and encryption to implementing best practices and leveraging emerging technologies, the path to robust digital security requires continuous learning and adaptation.

The challenges we face are significant, but so too are the opportunities to create more secure, resilient systems. By staying informed, implementing comprehensive security measures, and fostering a culture of security awareness, we can work towards a digital future that balances innovation with protection.

As individuals and organisations, we must recognise that digital security is not a destination but a journey. It requires ongoing vigilance, adaptation to new threats, and a commitment to protecting not just our own data but also the data entrusted to us by others. In this interconnected digital world, our security practices have far-reaching implications, shaping the overall resilience and trustworthiness of our global digital ecosystem.

The national security, and economic stability of our nation is at stake, and the changing face of the battlefield means that bombs and guns are less utilised and now software warfare is truly on the rise.

The Author

Thomas Hamer served in the Royal Australian Navy from 2001-2006 as an Able Seaman Bosuns Mate, deploying to the Persian gulf as a .50 cal gunnery crew member, and was involved in border protection operations. Thomas is a technology professional working with the Amazon AWS cloud currently in banking technology in Australia. Thomas has a keen interest in autonomous aircraft, and flies his own drones making use of computers, and networking to pilot them, instead of flying by hand. Thomas is also a small boat sailor, and has travelled extensively, so far to 41 countries, and is trying to get to every one.

References

- Diffie Hellman Key Exchange: https://www.youtube.com/watch?v=NmM9HA2MQGI.
- Australian Legislation: https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/assistance-and-access-industry-assistance-framework.
- Crypto AG: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/.