Maritime Security in the Age of Digital Feudalism

A short rant on our relationship with technology

Constantine Macris

5NOV2020

Contents

0.1 Maritime Security in the Age of Digital Feudalism

0.1.1 whoami Constantine Macris

- Instructor US Coast Guard Academy
- Incident Response & Forensics Consultant
- Student US Naval War College
- Security Innovator

Figure 0.1: New England

I spend most mornings teaching, most days researching maritime security, and most nights hacking about on one of a million projects, responding to an incident, or taking classes at the US Naval War College. As a security professional, I keep pretty busy. Before I get started, I want to take a moment to thank the great folks at Dispel who made this talk possible and the NZDIA for agreeing to let me talk. (My students would have advised against this, but here we are!) I have had the opportunity to work in both technical, leadership and teaching positions at various levels of industry and government. LinkedIn. My security journey started in 2002 at the United States Merchant Marine Academy. There, I joined the Network Security Team, which competed in various Capture the Flag and Cyber-Related competitions and was still in its infancy. I started to learn at that point that network security was a human problem. A very technical human problem, one that uses computers and gazillions of lines of code to create and subsequently solve. I also learned how to order pizza and make coffee for the team. By my final year I had gotten very good at making coffee and ordering pizza and had cemented my leadership position by moving computers around as needed. After graduation, I sailed commercially on my Coast Guard License for 8 years. I spent many nights on the ship while it was at the pier playing with systems and realizing that all those hours making coffee taught me a lot about how take over ship control systems in various different ways with an assortment of radios or micro-controllers. I then deployed to Africa with the Navy for a year, developed some remote sensing and reporting shipboard devices for use on environmental service vessels and ultimately ended up managing and rebuilding a large defense contractor's classified information systems. This led to similar work in the Navy, some consulting and finally to the Coast Guard Academy, where I make coffee and figure out how to take control of ships with various radios and micro-controllers. This time instead of being alone on a ship that I need to make sure works in the morning, I have a bunch of people who **need** to watch me hack around on things and I can break whatever I want, within reason.

Joking aside, today we are going to talk about:

- Digital feudalism and what that means to governments
- Building secure environments through the lens of government, maritime and industry
- How we can help future-proof and remain flexible in our implementation of technology to help guard against full reliance on a *feudal lord*
- How using open source tools can solve issues related to legacy systems.

0.1.2 Take Away

- Rethink about our relationship with technology
- How are we using technology to gain capability and efficiency

0.1.3 My Grandfathers Car

Figure 0.2: Cars

0.1.4 Digital Feudalism

- We live in an age of Digital Feudalism
- Technology has never been more accessible but we are growing further from it.

Leading cryptographer and security thinker Bruce Schneier has written a lot on the topic of security, **Applied Cryptography**. In 2013, Schneier wrote an article on Digital Feudalism in a publication called the *Multistakeholder Internet Dialog" called MIND 6. Schneier describes a cycle of technology where normal people of the future (today) need to align themselves with with a Digital Feudal Lord, like Google or Apple. That would enable that lord to protect that individual much like in feudal times.

In this case I have decided to join up under Lord Google and my lord provides me with a phone platform where I get free emails as long as my lord can read my emails. I get a world of information in my pocket as long as my lord can track where I am and what I am looking at. I get my most cherished family memories stored on my lord's computers as long has my lord can scan their faces and up sell me on photo albums.

At this point everyone is thinking what lord they live under: Amazon, Apple, Google, Facebook, Microsoft… The list goes on.

There are, however, those who can live outside this system. This is in reference to fights over strong encryption, mass government surveillance, etc. It points out that the masses will be using devices they don't understand, aligned with a digital lord, while criminals, dissidents, and other fringe groups will be able to understand technology enough to stand alone. The groups will always have the advantage of being able to innovate and adopt the latest technology quickly, while law enforcement, government, and other structured organizations will take time to catch up and implement new technologies.

From a government perspective, we need to ask:

- How can we adopt technology more rapidly to better keep up with adversaries? This important in information technology systems but CRITICAL for operation technology systems.
- How do we utilize technology in a way that gains the trust of our countries in support of a more secure and transparent future?

There are no easy answers, but I am working towards some solutions that I believe can help speed up adoption of technology.

0.1.5 Maritime System Security

- 80% of global trade travels by ships

Figure 0.3: Container Terminal

A.T. Mahan in “The Influence of Sea Power Upon History 1660-1783” describes how the history of seapower is linked to commerce. The original mission of navies was to protect Sea Lines of Communication or trade routes and police the oceans. With global GDP set to rebound after the coronavirus, we can expect shipping volumes to increase. While I am not here specifically to talk about commercial shipping, I am here to focus on the maritime aspects of technology. When I graduated from the US Merchant Marine Academy in 2006 we did not have a dedicated curriculum for Industrial Controls, Maritime Electronics, Networking or really any technology classes other than basic programming. Today things have gotten better but we are still only training mariners to be acquainted with technology, instead of having an intimate relationship with technology.

For those of you without a maritime background, some of the systems on a ship include Bridge systems to give the Captain information on where the ship is and where other ships and hazards are. The bridge systems can inform an Engine order system that controls the main propulsion of the ship. The rudder is usually controlled by a helm and autopilot system. Ships stability is controlled by a ballast system and power for the ship controlled by a generator system. Many times these systems are tied together because data from one system can help inform the better operation of another.

We look at OT networks as static, where we buy something and it does the job it was designed to do. It was never considered to have a patching cycle or traditional 5 year lifespan. We do not consider it to be part of an interconnected network of devices that assist in the operation of the ship. Additionally, in order to run many OT networks, we need the support and connection to IT networks. In a static factory

this connection between IT and OT networks can be defined where one workstation is responsible to bridge that gap, with reliable connectivity on one side and the secured OT environment on the other. In maritime, the difference is that there usually is not the benefit of having a stable connection and the ability for specific techs to be able to jump on the OT network when needed (you are on a ship). Many times we do not even consider these networked connected devices to be a threat.

When I generally talk about the detailed hoops I need to jump through to exploit some systems, many individuals say “yea well when is that going to happen” and for the most part, I admit it is difficult, and to execute one would need a concerted plan and would have a low likelihood of execution. That being said, the risk is not just the likelihood of something happening but the severity of what the result could be. I worked on ships in New York Harbor, and I can guarantee that the severity of a 360 foot loaded tanker running into the Brooklyn Bridge would be catastrophic. A large container ship capsizing in the Norfolk Thimble Shoal Channel or war ships losing control of a ship at a critical moment would also have a catastrophic effect.

In our Brooklyn Bridge example, the ship’s rudder system would need to be manipulated as the ship passes the bridge so that inputs could be read from the GPS location data and the rudder angle sensor could be manipulated to cause the helm system to correct the angle (to the wrong angle), causing which could cause the allision.

0.1.6 Capsize

Figure 0.4: Big Problems

0.1.7 Block Channel

Figure 0.5: So Tight

0.1.8 Warship

Figure 0.6: Collision

0.1.9 Bridge Systems

Figure 0.7: Bridge

We heavily utilized COTS in bridge systems based on old standards. A work around has been to add good encryption at the application layer and use AIS as a means to transfer that data but that is really only a partial solution to utilize a somewhat broken system. Any unauthenticated network (NMEA 2000, NMEA 0184, etc) is vulnerable to manipulation, which under certain circumstances could be catastrophic. Ship bridge systems are connected to various other shipboard systems including engine control, rudder

and ballast systems. As we start building these networks to enable additional functionality, it opens up new ways to move around networks and create various different effects. Many times, we find ourselves fighting to get systems to just work let alone being able to properly secure them. From that point, most leadership has a hard time understanding the technology enough to properly scope the problem. The idea of Digital Feudalism, in my mind it is the tendency of most people to gravitate towards simply using technology and not really understanding how all the parts that got us here work.

0.1.10 Fostering the next generation's understanding of technology

- Work to make technology attainable
  - Hardware Hacking
- Give everyone tools they can use for a lifetime
  - Open Standards / Open Source
- Adopt and implement the latest technology
  - Use automation like Ansible and Terraform
  - Deploy to cloud or on-prem

During my time at the US Coast Guard Academy I have worked to expose future officers to specific foundational skills that allow them to gain an understanding of technology at all levels. This includes pulling communications off a wire using a logic analyzer, injecting packets onto networks and decoding unknown protocols. We work to develop fluency with all levels of technology where students can choose the best system for their use-case. The goal is to provide future decision makers to have insights into technology choices and break the day to day reliance on our digital feudal lords.

We attempt to use open standards and open source so that students can take tools with them and develop their own labs upon graduation to test and prove out ideas. Through this process, future leadership will be more likely to be able to simulate a scenario before it becomes a problem.

Most importantly, we attempt to ride whatever the latest wave is and be prepared to pivot with technology. As with elections, it is dangerous to place bets on winners too soon! For that reason we use the best available technology, knowing that it may not emerge as a well supported standard and we must be able to pivot as new tech becomes available. We store our material and source as code so it is easy to view, edit and track changes of state, and we work to separate content from presentation in order to create a holistic approach to learning and solving problems.

0.1.11 My Research

- Building systems that build systems

- Automate the process of deployment, configuration, accreditation and authorization (A&A)
- Deploy specific environment for a purpose, save needed data then destroy them

To end off I want to take a moment on what I work on in my spare time. As you can imagine I am a firm believe in process. I have grown up in the NIST 800-53 control framework and believe that proper documentation and authorization and accreditation is pivotal to building robust systems. I find that process is far too slow to keep up with the criminals (in our Digital Feudalism example) or simply to be able to implement the newest technologies and I think a lot of risk remains by having systems that are existing after they are no longer needed.

I build systems that build systems. I use NIST principals to build a system for a job that can create a A&A package during deployment. The system is described as code using automation tooling. That state can be verified and managed, and during the deployment process all needed A&A information can be input into Security Plan templates so after a few minutes a new environment is ready for use. This can occur in the cloud, or in various different on-prem locations (Boats, Ships, UAV…).

The goal is to make old technology go away and start fresh with each new mission.

0.1.12 The Dream

- Evolving Target Defense
- Purple Team Alpha

Depending on where my research takes me I intend to give my systems the ability to deploy mirror environments on the same hardware utilizing virtualization and software-defined networking. As needed, services can be migrated in near real-time to the mirrored system to allow a potential event to be observed. This can gather TTPs and data on the “event” while continuing operations. I think of this technology as **Evolving Target Defense** where what we learn from one mission would inform the configuration of the next. Constantly moving, constantly growing and constantly improving. I have been working with the folks at Dispel and their Project Pangolin on this concept and look forward to some small scale deployments to give to my students to try to break!

0.1.13 Conclusion

- We need to realize our reliance on our feudal overlords
- To keep up with the fringe groups we must promote a different relationship with technology
- Break stuff (in a lab)

I hope we all realized that we do fall under some digital feudal lord and that it has opened up our understanding on how we think about our relationship with technology. I wanted to use the lens of

maritime and my experience to talk a little about how I plan to start to holistically tackle these problems. I understand it involves a completely new way of thinking about our relationship with technology and breaking down the old way of doing things and thinking and moving towards what is a very uncertain and confusing future.

0.1.14 Content

- Static Content at nz.hacking.fans
- PDF Handout
- Slides