Cybersecurity in the Residence: An Application-Based Actor-Network Theory Framework

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science, School of Engineering

Sean Benish
Fall, 2021

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Signature Sean Benish Date 12/15/2021
Sean Benish

Approved _____ Date 12/15/2021
Richard Jacques, Department of Engineering and Society

Cybersecurity in the Residence: An Application-Based Actor-Network Theory Framework

STS 4600 Research Paper

Sean Benish

November 8, 2021

Contents

1 Introduction

In 2016, Balzacq and Cavelty contextualized cybersecurity as the formation of a stabilized actor-network. In their paper, they describe how cyber threats target parts of this stable system and cause depunctualisation—the transition into an unstable network. With this framework, the researchers applied their model to understand the political implications of cyber incidents, such as cyber-attacks, a hole now filled. In cybersecurity, another hole remains mostly empty—an understanding on how the average person approaches cybersecurity. Researchers have already examined outcomes of cybersecurity across age groups Jiang et al. (2016) and provided tools for managing their cybersecurity (Alotaibi et al., 2020), but an in-depth, generalized model for understanding recognition, response, and resolution to cyber-incidents does not exist. Therefore, this research intends to identify what actors currently exist and how they interact to form cybersecurity in the home, an insecure haven (Furnell & Moore, 2014).

2 Methodology

This paper constructs an actor-network theory framework for residential cybersecurity. With this framework, one can better analyze cybersecurity trends and cybersecurity events to identify key actors. Understanding the attack path, data flow, and response phases aids this analysis. After the model is constructed, example cases will apply this framework to understand the actors at play, the flaws in the network, responsible parties, and suggested courses of action.

Note that this paper focuses on internet usage and trends in the United States. The social and legal context of the internet varies from country to country. Therefore, parts of the actor network may need to change from nation-to-nation. If needed, adjust these frameworks accordingly.

3 Framework and Usage

3.1 Physical Network

In order to understand cybersecurity, one must understand the computer networking infrastructure. To do this, five actor-networks represent the layers of communication: the resident (user), "human-interface device" (HID), local-area network (LAN), wide-area networks (WANs), and endpoints. Figure 1 lays out these connections into an initial network. First, the description and physical actors will be defined. Then, a deeper analysis of the networks will be performed.

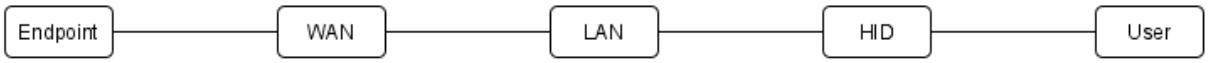


Figure 1: High-Level Description of the Resident-View of the Internet

3.1.1 Actor Overview

The resident represent an individual manipulating devices to interface with the Internet. Thus, the "human-interface device" (HID) represents a grouping of devices that translates inputs from a person and into digital signals. Note that this paper uses a different definition of a "human-interface" device than the traditional definition (see (Techopedia, 2019) for more details). Common "human-interface devices" include laptops, smartphones, desktops, and IoT devices.

Devices do not connect directly to the Internet, but require intermediate devices to facilitate communication. The "local-area network" (LAN) includes these devices as well as HIDs. LANs (in general) include network switches, hubs, and at least one router. In most home environments, a wireless LAN (WLAN) also

exists via a wireless access point, allowing for Wi-Fi connection. Furthermore, routers typically carry at least one access point, sufficient for most home networks. As the homes of today focus more on their wireless networks rather than their wired, Wi-Fi repeaters and extenders play a more prevalent role. Note, however, some apartments still use wired equipment like switches to connect all of the tenets in a building. At the end of the LAN, a router and modem (typically integrated into one device) manage communication over the Internet-Service Provider's (ISP) network.

Outside of the home lies "wide-area networks" (WANs). A resident has little control over WANs, but residents may be able to choose their closest WAN by selecting an ISP. ISPs connect homes to other WANs like the Internet. WANs all have the goal to transmit as much data as possible to their respective destination as quickly as it can (Cahn, 1998). WAN designers juggle many factors including estimated bandwidth, cost, hardware capabilities, and latency into the design of the network (Cahn, 1998). To facilitate communication, WANs use WAN-capable routers to quickly send traffic over large distances. Many other factors exist within the large scope that is in the WAN (see the intercontinental links), but their inclusion is not as useful to home cybersecurity. Availability is the number-one goal for these networks, so this report solely focuses on their ability to facilitate communication.

A user connects to the Internet with the intent to communicate. Therefore, this last group, the endpoints, represents *who or what* the user communicates to. Common activities on the internet include checking email, direct messaging, voice calls, gathering information, education, commerce, social media, and entertainment (Lebo, 2018). Endpoints connect people and information to the user. For example, online commerce sites like Amazon or eBay (in general) allow sellers to post information about products that users can access through the endpoint. Similarly, email servers receive messages to the user and store them for later recovery.

To demonstrate the advancement of the model, Figure 2 adds to the initial design in Figure 1.

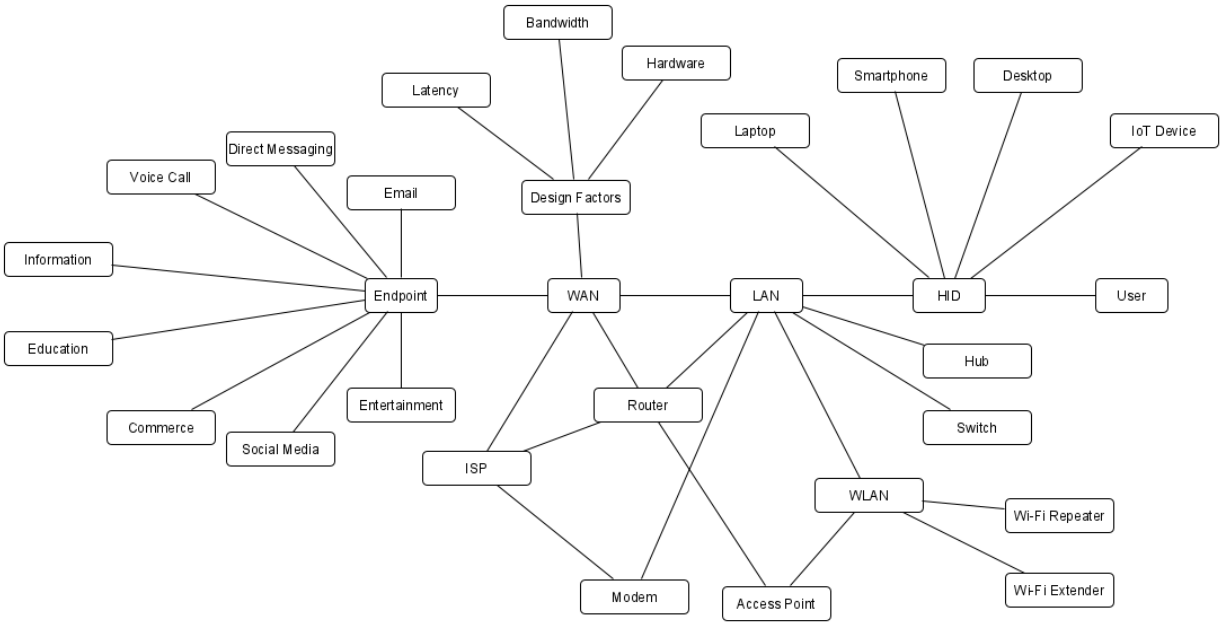


Figure 2: Physical Overview of the Resident-View of the Internet

3.1.2 Actor Analysis

With the general overview and the physical actors described, some of the influential actors associated with the networks can be added. The user, the start of the interaction, holds the most complexity of all

other networks described. Actors influencing the user primarily fall into three categories: HID, endpoint and security influencers. HID influencers tell which device the user will likely use, endpoint influencers suggest what endpoint a user will use, and security influencers represent actors that positively or negatively affect a user's cybersecurity practices. These influencers are too specific and/or numerous to identify, so this must be done while analyzing a cyber-incident.

"Human-Interface Devices" split their security influences among 3 primary networks: the hardware, low-level software, and application software. Hardware security represents a massive field of research, techniques, and designs used to ensure manufactures made the hardware as designed and to prevent tampering with said hardware. As of now, hardware security in the home plays no larger role than in most other industries. However, as the Internet of Things grows larger, embedded devices, generally unsecure (Anwar et al., 2017), will place a higher emphasis on this aspect. Therefore, hardware security should be recognized for future-proofing the model. Low-level software groups the software that makes the machine run regardless of application. This level includes operating systems for general-purpose computers, drivers, as well as application providers like web browsers. IoT devices may or may not have this layer. The final category, application software, encompasses the security aspects of the software that the user interacts with. Unlike low-level software, application software changes based on the endpoint, making security dependent the machine that runs the software *and* the endpoint.

As LANs primarily forward information, the security of this network depends on its ability to perform such an action and to resist tampering. As this layer is quite technical, many researchers and companies have identified threats. For an overview of these vulnerabilities, reference Feng Feng (2012) and Kiravuo et. al Kiravuo et al. (2013). Furthermore, note the ISP's influence over LANs (providing hardware).

Mostly outside of the user's control, the security of WANs depends on the design, maintenance, and research of these networks. Secure design represents the backbone of this layer's security. Maintenance ensures that outdated designs become replaced throughout the network. Research acts as the feedback loop—finding issues, responding the existing threats, and patching the holes.

Endpoints have numerous groupings. In the context of home cybersecurity, however, endpoints can be classified by their inclusion of secure activities and security risks. Secure activities include the authentication process, file sharing, communication, payment processing, sensitive information requests. Security risks involve secure activities as well as actions like data collection. Furthermore, the security of an endpoint depends on its owners and its operating policies.

As done previously, Figure 3 depicts this enhanced model of the security entities and relations relating to the physical network.

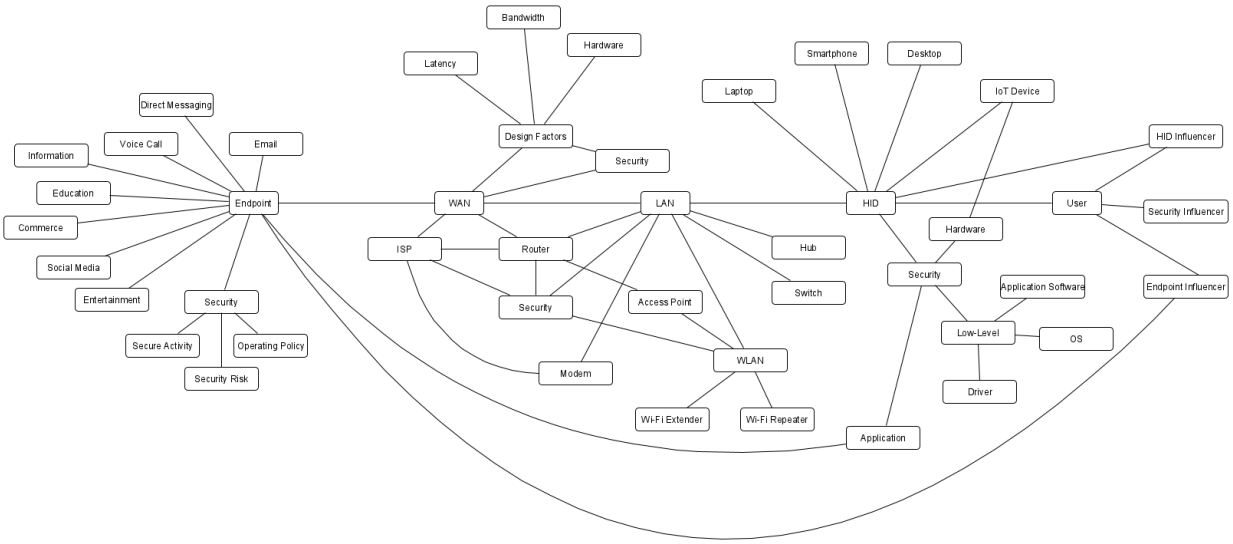


Figure 3: Security Overview of the Resident-View of the Internet

3.2 Attack Chain

While the physical network created an actor network for a user's communication to the internet, the attack chain actor-network defines the actors at play that cause a cyberattack to occur. In this model, all four actor-networks—attacker, vector, access, and target—must allow an attack through for one to occur (see Figure 4). Therefore, each link in the chain splits its relations into two categories: aiders and abettors. Aiders allow cyberattacks to occur while abettors resist the attack or decrease the damage done.

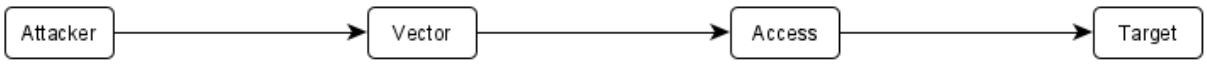


Figure 4: Attack Chain

3.2.1 Attacker

A cyberattack requires an attacker. The attacker network, thus, influences the creation, upkeep, and punishment of those executing cyberattacks. Bugeja et al. Bugeja et al. (2017) gives sources of cyberattacks: nation states, terrorists, criminal organizations, competitors, hacktivists, hackers, and thieves. They then classifies motivation for these malicious actors into curiosity, personal gain, terrorism, and national interests. In contrast, the legal system acts as the main threat to cybercriminals. In the United States, the U.S. secret service targets high-value criminals, with investigations led by the Immigration and Customs Enforcement's Cyber Crime's Center (C3) (Cybersecurity & CISA, 2018).

3.2.2 Vector

With an attacker, something needs to be attacked. The vector represents what the attacker targets to initiate the cyberattack. Critically, the attacker uses the actors of this network in unintended ways (an "exploit"). With cybersecurity design assuming insecure connections, most actors abet the chain. Furthermore, research can aid or abet, depending on who researchers (hackers vs. cybersecurity firm). Nearly anything can become a vector, so this network becomes well-defined either in retrospect or in predictions against

common attack paths. Common vectors targeting home users include routers, IoT devices (botnets), and personal computers (spyware, ransomware).

3.2.3 Access

Good security design assumes something is compromised. The access network holds all actors who enhance the security to a target if a system were to be compromised. For home networks, the depth of the access actor-network is not as large as in businesses. However, endpoint security serves as a (usually) high-security actor-network, as services need to protect themselves from attack. In home networks, a user's security comes from their network and their device. With home routers usually holding the sole wireless access point, the router handles most of the wireless security in addition to the border firewall to the WAN. Wireless security (in general) comes from the IEEE 802.11 family of protocols. The branded company, furthermore, holds some responsibility for the default firewall setting on the router, as most users cannot change these settings. The device itself then has the responsibility to handle any threats that passed through this layer. IoT devices typically will put a small veil of protection, but generally fall prey to cyberattacks (Anwar et al., 2017). Personal computers, on the other hand, have built-in firewalls and anti-malware software to prevent and respond to threats as they arise. OS-level access control may also provide a level of security against unauthorized access from malicious actors.

3.2.4 Target

The target network records the end goal of attacks. This can include data to be swiped, malware to be installed, a network to bring down, etc. Factors in this network either increase or decrease the likelihood of a cyberattack causing damage. For example, many home networks are insecure (Furnell & Moore, 2014) but do not have enough valuable data to risk entry. Therefore, the lack of value in one's network deters hackers. However, the rise of insecure IoT devices gave value to these homes (Riggins & Wamba, 2015), as these devices can be used in bot-nets, large networks of small computers with a large cumulative processing power. Encryption and obfuscation also prevents or makes difficult finding valuable information.

To summarize these findings, Figure 5 depicts the attack chain with this analysis in mind.

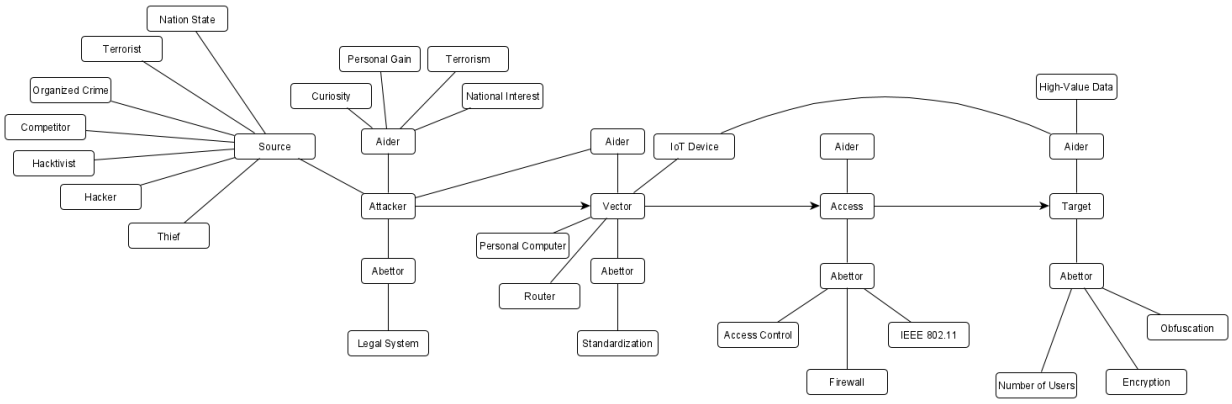


Figure 5: Extensive Attack Chain Actor Network

3.3 NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework Standards et al. (2018) breaks cybersecurity into five components: identify, protect, detect, respond, and recover. Each component represents and actor-network that, in total, secures the home from cyberthreats. The analysis

of these components will take the developed actor-networks for the physical network and attach chain into account. Figure 6 shows this initial framework, which will be detailed by the end of this section in Figure 8.

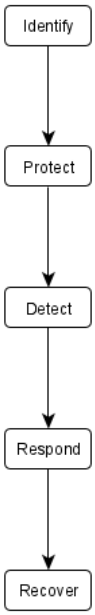


Figure 6: NIST Cybersecurity Framework

3.3.1 Identify

The identify network describes the actors and their relations that locate cybersecurity risks. For a residential context, this typically includes actors beside the user, as residents usually cannot locate weaknesses in their home network. Therefore, actors in this layer include those who influence the protective actions taken in the protection step: hardware manufacturers, software developers, malware signature databases, etc.

3.3.2 Protect

The protect network then targets actors, activities, and relations dealing the mitigating identified risks. In the context of the physical network, each device in the home plays some role in protection. Therefore, the networks associated with these devices and their software (manufactures, designers, maintainers, etc.) must be considered. Furthermore, endpoints also aid in protection. For example, an email server must protect a user's emails from unwanted eyes, so the server must have measures in place to prevent unauthorized access.

Moreover, the user's security influencers play a role in embedding good protective practices in users. Such practices include password management, anti-phishing, and safe web browsing. Thus, an individual's social network plays a significant importance in the home, where individual responsibility is more common than business-grade cybersecurity policy.

3.3.3 Detect

The detect network defines the actors who identify cybersecurity incidents. Businesses with intrusion-detection systems (IDS) can notify staff when a cybersecurity incident has occurred, yet residents do not have

this luxury. Therefore, endpoints, anti-malware software, and the user all perform detection of cybersecurity events.

Endpoints circumvent the issue of weak residential cybersecurity; the resident's data falls behind that business' security system. Therefore, detection of cyber incidents depends on that business' cybersecurity policy.

Inside the home environment, anti-malware software may prove vital for users to detect when a threat appears. For example, if spyware or a virus infects a personal computer, anti-malware software can detect these threats. Note, however, that IoT devices typically lack such software, so detection falls onto the last category.

The user acts as the last barrier to detect malware. As the average residential user is not technically savvy, detection of malware can go unnoticed. Therefore, a typical user detect malware when malware wants to be detected. Ransomware, for example, explicitly flaunts itself around after it caused damage to solicit payment.

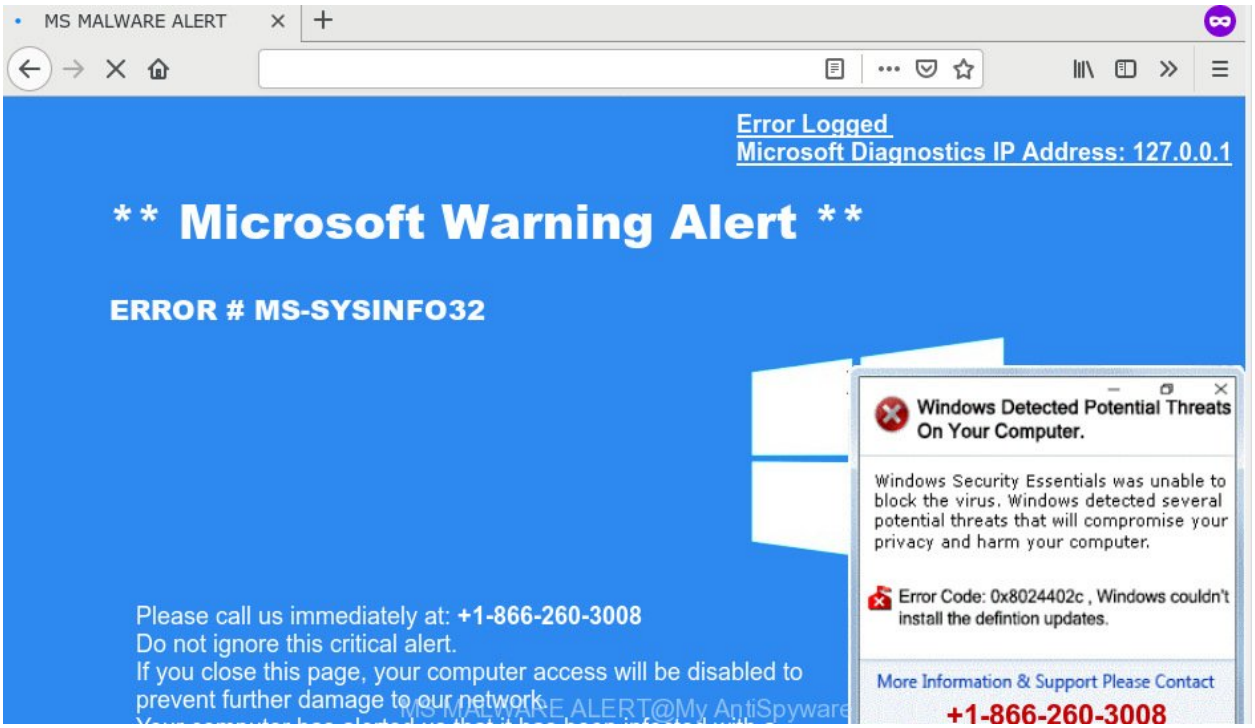
3.3.4 Respond

The respond network describes the actors that influence how a cybersecurity incident gets resolved. A "response chain", thus, represents a sequence of actors, the first beginning the response and the last ending it. As one must detect the incident before proceeding, the first links in the response chains are endpoints, anti-malware, and users.

When an endpoint begins the response, it may or may not go to another chain. For example, a security breach that did not affect a user's information represents a single-link chain. If user data was leaked, however, an endpoint may notify the user about the breach and give guidance on the next steps.

Anti-malware software typically attacks threats it detects unless specified by the user. This way, the system has a lower change of being compromised by the malware. Furthermore, security incidents may report to an authority's signature database—a store aiding the detection of malware—to boost the protection of other users.

Users may begin the chain, but rarely end it themselves. For the response chain to stop at the user, the user must know how to respond to the threat directly. Downloading an executable file, for instance, has a single-link response (erasing the file). However, other attacks require users to seek help elsewhere. This can include technical support, online forums, or even family members (Jiang et al., 2016). The tendency to seek out support, however, may be the exact target for a cyberattack. Malware scams exploit user's difficulty in assessing threats, often scamming users for personal information and/or money by pretending to be a direct line of support to resolve this phantom threat.



Source: https://www.myantispyware.com/

Figure 7: Fake Malware Scam

3.3.5 Recover

Finally, the recover network holds actors who prevent future occurrences and restore the structure of the actor-network. Connected to the end of the response chain, the last actor to respond becomes the first actor in the "recovery chain". Thus, the recovery chain encodes the different actions that actors use to reach an outcome.

Recovery chains fall into three broad categories: full recovery, partial recovery, and no recovery. Full recovery chains involve the complete elimination of the cyberthreat and its side effects. Thus, the event effectually did not occur. Anti-malware erasing malicious software before it executed represents full recovery. Partial recovery chains, thus, fail to erase all side effects of the malware. Removing spyware that already stole data falls into this category. Also, purchasing a new, uninfected device also falls into this category, as the malware will no longer operate. Finally, no recovery chains let the cyberattack win. These scenarios include account loss and complete loss of control of a system. The actors that fulfil these chains include technical support, data recovery, computer sales, and more.

Finally, Figure 8 incorporates these actors into an actor network.

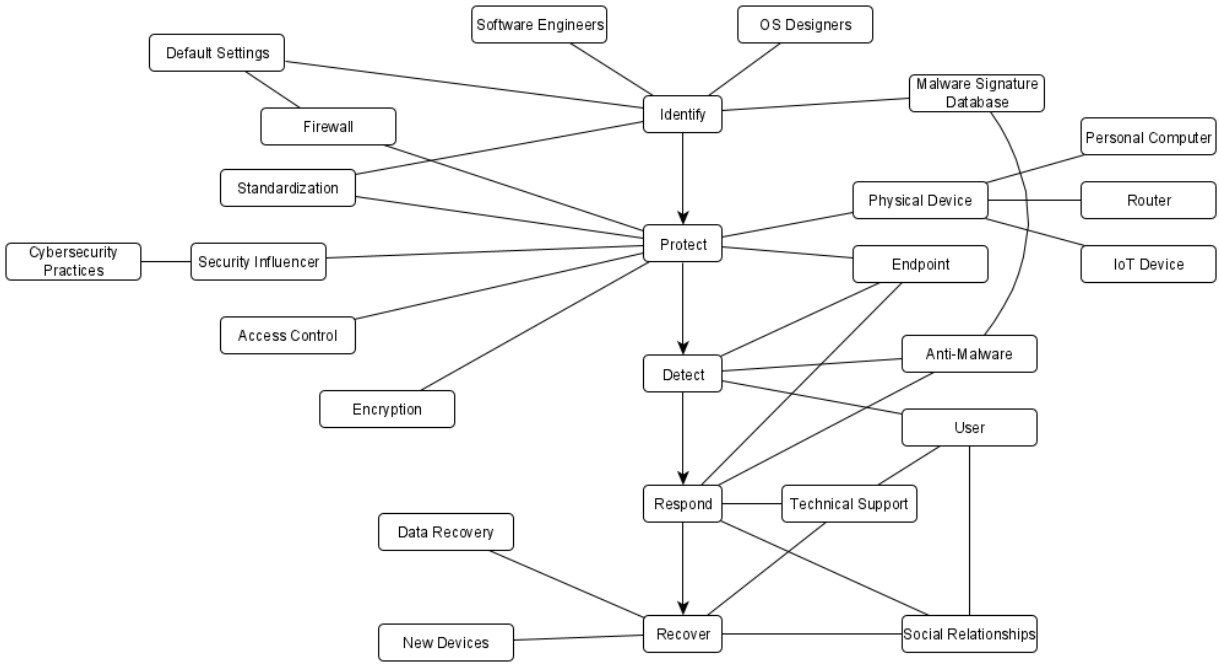


Figure 8: NIST Cybersecurity Actor Network

4 Application

With these three actor-networks as guidelines for analysis, two cyberattacks, the ILOVEYOU worm and Amazon Ring Wi-Fi exploit, will be analyzed under this framework. As these analyses will show, the framework guides the user to identify additional actors at play as well as how the fit in with the others. With this knowledge, ethical doctrines (i.e. deontological, consequential, and virtue-ethics) can be applied to place responsibility and resolve these holes.

4.1 ILOVEYOU

A Filipino student created a Visual Basic script in 2000 that would spread across the world and inflict an estimated $10 billion in damage (Poulsen, 2010). This worm, known as "ILOVEYOU", would target a user's Outlook program and forward copies of itself to saved contacts (Bishop, 2000). With the three actor networks, the path, communication, and response can be analyzed.

First, the attack chain will be understood. The worm ultimately targeted other users (to spread itself) but was not interested in anything outside of replication. To do this, the worm used a vector composed of the Windows OS, Internet Explorer, Microsoft Outlook, mIRC, and Visual Basic (Bishop, 2000). Access controls to break this vector (preventing user from writing to the registry, email detection of malware, anti-malware programs) were either circumvented or not present.

With the attack chain modeled, the dataflow over the physical network can be studied. First, the worm appears at one's email server (endpoint) before traveling to one's machine (HID). The "I LOVE YOU" message represents a portion of social engineering that exploits the general user's lack of cybersecurity knowledge. However, an external influence (such as having a non-Windows machine, and HID influencer) would prevent this attack from continuing (Bishop, 2000). Moreover, alternative email clients (endpoint influencer) would not stop the attack on this machine, but would prevent the worm's goal of proliferation.

The worm then used vulnerabilities in Outlook (application) and Windows (OS) to spread itself via email (endpoint).

With these connections in mind, one can now tackle the cybersecurity threat by applying the NIST framework. These can be separated into protective and recovery methods. In the protective method, this attack is added into the "identify" network and engineers design countermeasures ("protect"). For example, the long requirements for the attack chain suggest that if one of them were to block the attack, the worm would stop reproducing. Therefore, the developers of these applications and networks (primarily Microsoft in this case) should take action. Actions such as removing these emails from the outlook servers, enhancing access control, or blocking Visual Basic in Outlook could be viable options. In the recovery method, stopping the spread involves detecting infected machines and removing the worm. As the worm both exploits and embeds itself into the OS, Microsoft should assist users in repairing their machines.

4.2 Amazon Ring

In 2019, Bitdefender disclosed a vulnerability to Amazon in their Ring Video Doorbell. When configuring the device, the device creates an unprotected wireless network. A user can then connect to this network and enter the user's Wi-Fi network credentials. Because this is sent over an unencrypted Wi-Fi channel, any attacker can sniff the Wi-Fi packets to gain access to the home's wireless network (Bitdefender, 2019).

First, the attack chain will be identified. The Wi-Fi credentials for the home network were the targets of this attack, using the doorbell (specifically it configuration process) as the vector. In this situation, no access layer was present for this category of attack (which is why it went through).

Next, the physical network will be generated. The Amazon Ring and the smartphone app lay as HIDs in the network. The two HIDs interact with one another during setup. Additional connections are not necessary for this analysis.

Initially, the attacker only has influence on the Amazon Ring's actor-network. The attacker then sends data that causes the user to perceive the device as offline. When the user reconfigures the device, the user sends network credentials and the attacker saves then. The user then returns to normal activity, but the attacker has access to the LAN.

These two networks give information into how to respond to this attack. First, the attack chain identifies the target as network credentials, which turns this attack into a vector for a different threat. In addition, the lack of an access link identifies one of the key holes in the design—the assumption that information is secure. Furthermore, the access link suggests that changing the configuration of the setup Wi-Fi network may be sufficient for stopping this attack. From the perspective of the attack chain, preventing this attack requires either removing the vector (preventing the attacker from making the device appear offline), reinforcing access (ensuring the setup Wi-Fi network uses secure standards), or reinforcing the target (preventing the attacker from understanding the credentials).

Next, the physical network suggests how to fix the attack by using the data flow. First, communication exists within the LAN, so responsibility falls with actors within this actor-network. Next, the attacked data channel connected the smartphone app to the Ring. Furthermore, this channel was fooled into believe the device was offline then hijacked to take sensitive information. Therefore, the responsibility of preventing the attack falls on the parties responsible for communication between these devices. In this case, Amazon represents both parties.

Finally, the NIST framework can be used to suggest how Amazon can resolve this problem. First, this threat needs to be addressed in the "identify" stage. Then, the attack needs to be thwarted at through protection and/or recovery. With a protective method, the device can be updated with the previous suggestions to remove the vulnerability. With a recovery method, the device should be able to identify when the attack starts (i.e. the fake data is sent). Then, it can respond by notifying the user of the attack in progress and suggest further action.

5 Conclusion

With a lack of understanding about cybersecurity for an average residential user, this residential cybersecurity framework identifies the common actors and establishes actors along an attack path (attack chain), data flow (physical network), and response phases (NIST). When analyzing security events, the physical and attack chain help categorize and organize the event. Then, the NIST framework provides information on how to prevent future attacks as well as paths to resolve and recover from events. With this tool, stakeholder analysis of the home's cybersecurity become a lot easier.

6 References

Alotaibi, F. G., Clarke, N., & Furnell, S. M. (2020). A novel approach for improving information security management and awareness for home environments. , *ahead-of-print*. Retrieved 2021-03-23, from https://www.emerald.com/insight/content/doi/10.1108/ICS-05-2020-0073/full/html doi: 10.1108/ICS-05-2020-0073

Anwar, M. N., Nazir, M., & Mustafa, K. (2017). Security threats taxonomy: Smart-home perspective. In *2017 3rd international conference on advances in computing,communication automation (ICACCA) (fall)* (pp. 1–4). doi: 10.1109/ICACCAF.2017.8344666

Bishop, M. (2000). *Analysis of the ILOVEYOU worm.* Retrieved from AnalysisoftheILOVEYOUWorm (Publication Title: University of California at Davis)

Bitdefender. (2019). *Ring video doorbell pro under the scope.* Bitdefender.

Bugeja, J., Jacobsson, A., & Davidsson, P. (2017). An analysis of malicious threat agents for the smart connected home. In *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)* (pp. 557–562). doi: 10.1109/PERCOMW.2017.7917623

Cahn, R. S. (1998). "hello world" of network design. In *Wide area network design: Concepts and tools for optimization* (pp. 11–21). Morgan Kaufmann.

Cybersecurity, & CISA, I. S. A. (2018). *Combating cyber crime.* Cybersecurity and Infrastructure Security Agency CISA. Retrieved from https://www.cisa.gov/combating-cyber-crime (Publication Title: Cybersecurity and Infrastructure Security Agency CISA)

Feng, P. (2012). Wireless LAN security issues and solutions. In *2012 IEEE symposium on robotics and applications (ISRA)* (pp. 921–924). doi: 10.1109/ISRA.2012.6219343

Furnell, S., & Moore, L. (2014). Security literacy: the missing link in today's online society? , *2014*(5), 12–18. Retrieved from https://www.sciencedirect.com/science/article/pii/S1361372314704919 doi: https://doi.org/10.1016/S1361-3723(14)70491-9

Jiang, M., Tsai, H.-y. S., Cotten, S. R., Rifon, N. J., LaRose, R., & Alhabash, S. (2016). Generational differences in online safety perceptions, knowledge, and practices. , *42*(9), 621–634. Retrieved from https://doi.org/10.1080/03601277.2016.1205408 (Publisher: Routledge _eprint: https://doi.org/10.1080/03601277.2016.1205408) doi: 10.1080/03601277.2016.1205408

Kiravuo, T., Sarela, M., & Manner, J. (2013). A survey of ethernet LAN security. , *15*(3), 1477–1491. doi: 10.1109/SURV.2012.121112.00190

Lebo, H. (2018). *The world internet project international report* (9th ed.; M. Dunahee, Ed.). Center for the Digital Future. (Publication Title: The World Internet Project International Report)

Poulsen, K. (2010). *May 4, 2000: Tainted 'love' infects computers.* Wired. Retrieved from https://www.wired.com/2010/05/0504i-love-you-virus/ (Publication Title: Wired)

Riggins, F. J., & Wamba, S. F. (2015). Research directions on the adoption, usage, and impact of the internet of things through the use of big data analytics. In *2015 48th hawaii international conference on system sciences* (p. 1531-1540). doi: 10.1109/HICSS.2015.186

Standards, N. I. o., Technology, & N/A. (2018). *Framework for improving critical infrastructure cybersecurity.* National Institute of Standards and Technology. (Publication Title: Framework for improving critical infrastructure cybersecurity)

Techopedia. (2019). *What is a human interface device (HID)?* Techopedia. Retrieved from https://www.techopedia.com/definition/19781/human-interface-device-hid (Publication Title: Techopedia.com)