




Anatomy of an Internet Hijack And Interception Attack: A Global And Educational Perspective

Ben A. Scott
Edith Cowan University

Michael N. Johnstone
Edith Cowan University

Patryk Szewczyk
Edith Cowan University

Follow this and additional works at: <https://commons.erau.edu/adfsl>

 Part of the [Aviation Safety and Security Commons](#), [Computer Law Commons](#), [Defense and Security Studies Commons](#), [Forensic Science and Technology Commons](#), [Information Security Commons](#), [National Security Law Commons](#), [OS and Networks Commons](#), [Other Computer Sciences Commons](#), and the [Social Control, Law, Crime, and Deviance Commons](#)

Scholarly Commons Citation

Scott, Ben A.; Johnstone, Michael N.; and Szewczyk, Patryk, "Anatomy of an Internet Hijack And Interception Attack: A Global And Educational Perspective" (2022). *Annual ADFSL Conference on Digital Forensics, Security and Law*. 9.

<https://commons.erau.edu/adfsl/2022/presentations/9>

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.

EMBRY-RIDDLE
Aeronautical University™
SCHOLARLY COMMONS

(c)ADFSL



ANATOMY OF AN INTERNET HIJACK AND INTERCEPTION ATTACK: A GLOBAL AND EDUCATIONAL PERSPECTIVE

Ben A. Scott Michael N. Johnstone Patryk Szewczyk

Edith Cowan University, Perth WA 6027

{ben.scott,m.johnstone,p.szewczyk}@ecu.edu.au

<http://www.ecu.edu.au>

ABSTRACT

The Internet’s underlying vulnerable protocol infrastructure is a rich target for cyber crime, cyber espionage and cyber warfare operations. The stability and security of the Internet infrastructure are important to the function of global matters of state, critical infrastructure, global e-commerce and election systems. There are global approaches to tackle Internet security challenges that include governance, law, educational and technical perspectives. This paper reviews a number of approaches to these challenges, the increasingly surgical attacks that target the underlying vulnerable protocol infrastructure of the Internet, and the extant cyber security education curricula; we find the majority of predominant cyber security education frameworks do not address security for the Internet’s critical communication system, the Border Gateway Protocol (BGP). Finally, we present a case study as an anatomy of such an attack. The case study can be implemented ethically and safely for educational purposes.

Keywords: Cyber crime, cyber espionage, internet security, education

1. INTRODUCTION

The Internet’s underlying vulnerable protocol infrastructure, such as the Border Gateway Protocol (BGP) and Domain Name System (DNS), is a high-value target for cyber crime, espionage and warfare operations (Demchak & Shavitt, 2018; Smith, Birkeland, McDaniel, & Schuchard, 2020). For instance, Internet ‘hijack’ attacks have resulted in large volumes of the world’s global Internet traffic being re-routed through state-owned telecommunications operators, where cyber-surveillance, espionage, malicious injection and retrospective forensic analysis can be utilised (Demchak & Shavitt, 2018; Smith et al., 2020; Mitseva, Panchenko, & Engel, 2018).

The Internet is not only an implementation of technological and topological concepts, it is also a complex socio-economic system, thus infer-

ences about its operation based simply on physical topology can be flawed (Alderson, Doyle, & Willinger, 2019; Motamedi et al., 2019). Business and geopolitical factors can impact routing decisions, with some high-precision BGP attacks targeting differences between business and peering relationships for Internet routing behaviours (Birge-Lee, Wang, Rexford, & Mittal, 2019).

Within the domains of international relations and law, geopolitical Cyber Norms have been developed via the United Nations (UN), to help create stability in cyber space (see Figure 1); this ‘stability’ often refers to state-actors and geopolitical relations stability rather than technical stability (Broeders & Cristiano, 2020; Meyer, 2020). Concurrently, the non-state actor stakeholder community that operates and maintains global internet connectivity has developed its own set of technical norms to create a sta-

ble and secure routing system (Hesselman et al., 2020; Testart, Richter, King, Dainotti, & Clark, 2019). For example, the Internet Society’s Mutually Agreed Norms on Routing Security (MANRS) program and platform consists of non-state actors such as Tier-1 networks, Internet Service Providers (ISPs), Internet Exchange Points (IXPs), Content Delivery Networks (CDNs) and Cloud providers that represent critical Internet infrastructure and services on which (often sensitive) system operations and transactions take place (Testart & Clark, 2020; Freedman et al., 2018).

Invariably it will be Security Operation Centre (SOC) analysts and Digital Forensics and Incident Response (DFIR) professionals, staffed within these organisations and others, such as Computer Security Incident Response Teams (CSIRTs or CERTs), that ultimately form the front-line of practical implementation (and perhaps enforcement) of Internet and BGP routing security norms. The operationalisation of global Cyber Norms will need to implement comprehensive and robust Internet routing security measures to combat the increasingly sophisticated and surgical attacks on underlying protocols (e.g., BGP). At the same time, it is important that educational institutions and training providers keep pace and deliver adequate curricula in these domains. As will be discussed in Section 6, several predominant cyber security curricula do not adequately address BGP security.

This paper briefly considers global attempts to create norms for responsible behavior in cyber space, where practically all agreed-upon norms for responsible cyber behaviour relate to, and are impacted by, the Internet’s underlying protocol infrastructure (Section 3 and 4). We also discuss a non-state entity practical implementation framework (Section 5). Secondly, we describe a number of increasingly surgical attacks that target the underlying vulnerable protocol infrastructure of the Internet (Sections 6 and 7). Finally, we evaluate how several education frameworks may (or may not) address BGP in curricula and present a case study for a simulated surgical attack (Sections 8 and 9). The case study



Figure 1: The 11 UN Cyber Norms
(UN Cyber Norms, 2021)

can be implemented ethically and safely for educational purposes.

2. BACKGROUND AND MOTIVATION

When the Internet was conceived, priority was placed on the immediate functional and operational requirements; the evolution of significant network protocol innovation is inextricably linked to the history of the Internet. For example, the Transmission Control Protocol and Internet Protocol (TCP/IP), core to inter-networking today, developed from work at the Defense Advanced Research Projects Agency (DARPA) (Cerf & Kahn, 2005).

BGP is the default inter-domain routing protocol for the Internet, connecting large networks, or Autonomous Systems (ASes), together by routing traffic accurately and efficiently. ASes are inter-networked routing domains administered by a single authority (Boitmanis, Brandes, & Pich, 2008). These structures are not physically or geographically bound but rather formed by organisational, corporate and political factors (Ball, 2020; Roughan, Willinger, Maennel, Perouli, & Bush, 2011). Similar to IP addressing, ASes have unique identification numbers (an ASN). Each AS represents a range of IP addresses and the attributes of BGP provide efficient routing mechanisms for inter-networking.

The strategic objectives of any AS (and any organisation using the Internet) are reliant on Network Reachability Information (NRI) and connectivity. BGP is also fundamentally based on trust and is, therefore, insecure (Cho, Fontugne, Cho, Dainotti, & Gill, 2019; Smith et al., 2020).

There is no requirement for cyber-attacks to specifically target BGP infrastructure for there to be destructive impacts on the services provided by the protocol. For example, there is evidence of cyber-attacks of an indirect nature that have caused BGP disruption (e.g. the Slammer and WannaCry malware); the outcome of these malware incidents impacted ASes with intensified BGP activity that ultimately overloaded the Internet. For example, on the day preceding the Slammer worm incident, the BGP announcement average was approximately 47 updates per prefix in contrast to 4500 updates per prefix during the attack (Lad, Zhao, Zhang, Massey, & Zhang, 2003; Moriano, Hill, & Camp, 2019).

The estimated annual financial impact of cyber-incidents falls within the hundreds of billions through to trillions of dollars range (Srinivasan, 2017). For example, the NotPetya malware is considered one of the most globally significant and financially devastating cyber-attacks in history, with quantifiable losses ranging from the low billions up to ten billion dollars in directly quantifiable damage (Greenberg, 2018; Gisel, Rodenhäuser, & Dörmann, 2020). Targeted BGP attacks can also be rapid and deliver cyber-criminals a quick financial windfall. For example, in 2022, malicious actors stole approximately two million dollars worth of cryptocurrency from a South Korean cryptocurrency platform using a BGP hijack attack (Cimpanu, 2022; Birge-Lee et al., 2021). The attack was well planned, though this form of hijack has been previously shown to be executed in only 35-seconds (Birge-Lee, Sun, Edmundson, Rexford, & Mittal, 2018).

There also exist geopolitical motivations for, and impacts from, cyber-attacks. Postmortem analysis of the NotPetya malware attack revealed geopolitical conflicts between Russia and Ukraine as the primary motivation for its execution, rather than any specific financial wind-

fall (Buchanan, 2020). The Stuxnet attack was similarly geopolitical in nature though it focused on the Iranian nuclear facilities program (Buchanan, 2020). The use of state-owned telecommunications companies (Telcos) to target BGP vulnerabilities, hijack the Internet backbone, intercept Internet traffic, and circumvent international agreements, is further evidence of geopolitical tensions and disagreements that influence cyber security (Demchak & Shavitt, 2018).

Whilst previous cyber-focused international negotiations (e.g., the 2015 ‘Xi-Obama agreement’) sought to specifically prohibit direct attacks on enterprise networks, the negotiations failed to address the capacity to directly attack an underlying internet protocol (e.g., BGP). For example, at the time of the Xi-Obama agreement, China Telecom had ten points of presence (PoPs) in the Internet backbone of the USA; the agreement did little to reduce hijacking activity of such infrastructure four years later, when traffic was re-routed through China Telecom. Internet routing or forwarding attacks can affect service quality on the very foundation of the Internet, and this represents significant need to address these matters. The ability to secure BGP against large Internet-scaled attacks can improve the global cyber security posture for cloud services, critical infrastructure, cyber-physical systems, government agencies, network operators, ISPs, IXPs, and CDNs.

3. A GLOBAL APPROACH TO CYBER CRIME, ESPIONAGE AND WARFARE

The UN has sought to address the challenges of irresponsible cyber activity via several state-based processes. The UN Group of Governmental Experts (GGE) 2015 report was endorsed by all countries in the UN General Assembly Resolution A/70/237 as part of the UN Framework of Responsible state Behaviour in Cyberspace. The UN Open-ended Working Group (OEWG) and the GGE are two complementary processes that build on the existing UN framework for the implementation of UN Cyber Norms.

Both the OEWG and GGE achieved consensus in 2021, an outcome that was widely considered significant; with 193 nation states having reached consensus as part of OEWG and nations such as the USA and Russia (in addition to 23 other countries) also reaching consensus within the GGE process (Gold, 2021; *UN GGE and OEWG*, 2021). There are 11 agreed-upon Cyber Norms for responsible state behaviour and the OEWG noted the need to make clear how norms can be practically implemented (Figure 1).

In both geopolitical and technical contexts, most (if not all) mutually agreed-upon norms for responsible cyber behaviour pertain to the Internet backbone and core infrastructure (Feakin & Weaver, 2020; Maurer, 2020). Whilst the terms ‘public core’ and ‘internet backbone’ continue to be debated from both perspectives (geopolitically and technically), the stability and security of the Internet infrastructure is important to the resilience of critical infrastructure, global e-commerce and election systems. Critical to the stability of Internet infrastructure is the global inter-domain routing protocol (BGP) and an insecure and unstable Internet BGP will result in a failure to practically implement and enforce recent global progress on responsible cyber behaviour. Security applications must address the multi-dimensional nature of the Internet and BGP attacks.

4. THE FRONTLINE

The challenge of securing the protocol underpinning the Internet is complex. The security demands range from incident response, and protection through to the need for the large-scale distributed system to have formal security verification, and ultimately both origin and path validation. Inevitably, the practical implementation and application of any global cyber norms and agreements would need to be executed throughout the Tier-1 networks, ISPs, IXPs, CDNs and ASes that represent the infrastructure on which critical system operations and transactions take place (Testart & Clark, 2020; Freedman et al., 2018). Several of these entities are members of the MANRS initiative (Kirkpatrick, 2021; Freed-

man et al., 2018).

Invariably it will be network operators (NOs), staffed within these organisations and others such as Computer Security Incident Response Teams (CSIRTs or CERTs), that ultimately form the frontline of practical implementation (and perhaps enforcement) of internet and BGP routing security norms. An outline of the general categories of currently available cyber security techniques and applications for internet security engineering is provided in the following sub-sections. An analysis of the Cyber Norms within the context of MANRS as a practical implementation framework is described in Section 5.

4.1 Routing security policy and governance

The MANRS members formally agree to take routing security policy and governance (RSPG) actions to achieve Internet routing stability and security (Freedman et al., 2018; Testart & Clark, 2020). These include coordination to facilitate global operational communication and coordination between NOs, filtering to prevent the propagation of incorrect routing information, validation of routing information on a global scale and anti-spoofing to prevent traffic with spoofed source IP addresses (*MANRS Observatory*, n.d.). MANRS also requires additional and specific actions dependent on the member category. For example, an IXP is required to also facilitate global operational communication and coordination and prevent the propagation of incorrect routing information, whilst specifically being required to also protect the peering platform, promote MANRS to the IXP membership and provide monitoring and debugging tools to members.

4.2 Internet route and path validation

As BGP was created at a time when security was not of primary concern; it was founded on an inter-network of trust, with the assumption that all networks are trustworthy (Al-Musawi, 2018; Testart et al., 2019). Inter-domain routing intelligence is the province of the control plane whilst

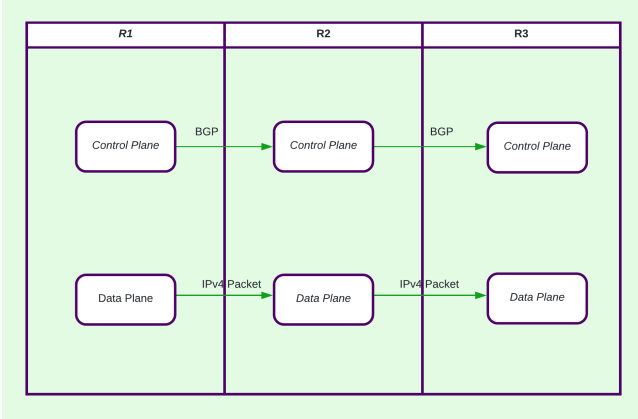


Figure 2: The control planes and data planes are responsible for different Internet functions

path forwarding is the data plane domain. There is no extant in-built validation for either plane in this critical global Internet communication protocol. Routing aims to find paths for pairs of end-hosts, whereas forwarding aims to direct packets from one end-host to another. Figure 2 illustrates the difference between the control and data planes. The latter has also been referred to as a hardware-layer that sees packets transferred across networks at line-speed, whilst the former has also been referred to as a software-layer and is responsible for establishing the routes between networks (via BGP) such that data plane information can be transferred successfully between networks (Bu et al., 2018).

4.2.1 Route Origin Validation

It is trivial for a malicious actor to announce prefixes they do not own (e.g., a BGP hijack). Therefore, the need for Route Origin Authorisation (ROA) and the advent of Resource Public Key Infrastructure (RPKI) have formed part of the Route Origin Validation (ROV) toolkit for security applications in the control plane (Chung et al., 2019; Kirkpatrick, 2021). The genesis of RPKI is found in the desire to verify BGP messages using cryptography with the premise of address space ownership certification (Chung et al., 2019). The practical deployment of ROV and RPKI as an application requires operators, in the first instance, to create ROA objects for cryptographically secured BGP announcement proofs.

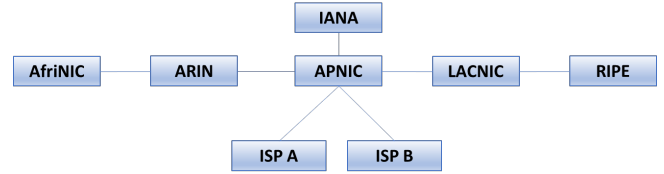


Figure 3: Internet addressing hierarchy

Due to the hierarchical nature of internet address allocation, RPKI certification is structured in parallel to this hierarchical system. As shown in Fig 3, the five Regional Internet Registries (RIRs) administering prefixes and AS numbers (ASNs) are the African Network Information Center (AfriNIC) for the African region, the Asia-Pacific Network Information Center (APNIC) for the Asian-Pacific region, Réseaux IP Européens (RIPE) for Europe, the American Registry for Internet Numbers (ARIN) for North America, and the Latin America and Caribbean Network Information Centre (LACNIC) for the Latin American and Caribbean regions. The adoption of RPKI as a security application has been steadily increasing (Rodday et al., 2021). We analyse ROV security application uptake by UN regions and RIRs.

While a quantitative analysis of RPKI adoption is beyond the scope of this paper, previous research has been conducted with uncontrolled and controlled experimental approaches (Rodday et al., 2021; Reuter et al., 2018). For the purposes of this paper, we desired to review RPKI adoption by UN region and sub-region for this preliminary analysis. The MANRS Observatory platform was developed to assist operators quickly identify internet routing incidents and provide verifiable attribution as to their nature and origin. The data analysed in this section was extracted from the MANRS Observatory, which ingests data from five well-known repositories: BGP Stream, CIDR Report, CAIDA Spoofer, RIPE Stats, and RPKI Validator.

RPKI adoption data across more than 79,000 ASes for the final quarter (October - December) of 2021 is shown in the following analysis. Like all internet topological research and BGP data sources, the Observatory is confronted with

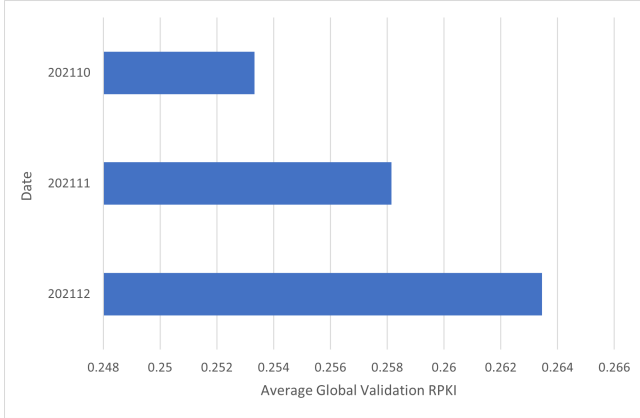


Figure 4: RPKI adoption

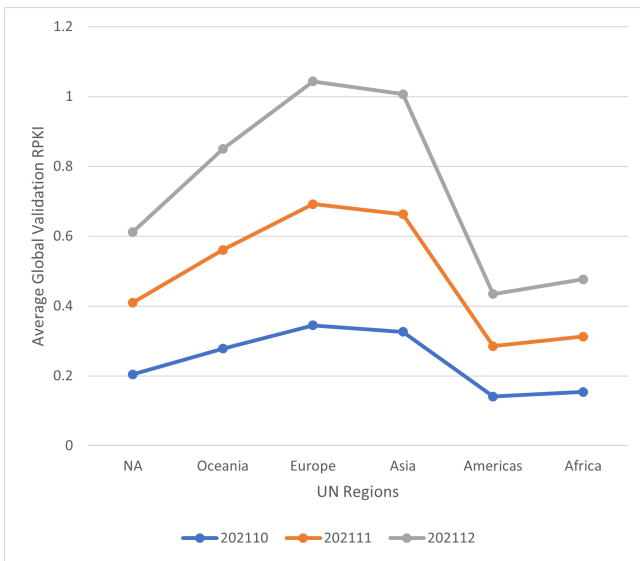


Figure 5: RPKI adoption by UN Region

ground truth challenges and suffers from a degree of false positives and false negatives in data classification; RPKI data ground truth is an ongoing research area and beyond the scope of this paper.

Analysing the MANRS observatory data for the final quarter period of 2021 we can see a continual increase in RPKI adoption (Figure 4). Despite challenges of ground truth, this is consistent with previous and recent research on RPKI adoption (Rodday et al., 2021). We can also see in Figure 5 that RPKI adoption has increased across all UN regions for the last three months of 2021.

Whilst this increased uptake of RPKI is consis-

tent with previous research, the practical and operational improvement from RPKI as a security application is reliant on the enforcement of RPKI via prefix announcement validation configuration and BGP announcement filtering per MANRS guidelines (Testart, Richter, King, Dainotti, & Clark, 2020). A deeper analysis into RPKI uptake is beyond the scope of this paper, however the techno-socio-economic distributed nature of this system must be considered in order to meaningfully assess this security application efficacy. We leave this to future research.

4.2.2 BGP Path Validation

Where routing aims to find paths for pairs of end-hosts, forwarding aims to direct packets from one end-host to another (Kim et al., 2014). The forwarding plane (also known as data plane) is also insecure. Route Origin Validation applications alone, such as RPKI, are not enough to secure BGP. Internet packet forwarding activity in the domain of the data plane has attracted research attention to address path vulnerabilities in Internet architecture (Legner, Klenze, Wyss, Sprenger, & Perrig, 2020).

Compromised routers can make forwarding decisions that deviate from the paths generated by the routing protocols; securing the routing process alone cannot guarantee correct packet forwarding (Bu et al., 2020). Additionally, endpoints have minimal to zero path property information and control; with investigations into origin path control, destination path control, and combinations of both, an active research area (Legner et al., 2020; Barrera, Chuat, Perrig, Reischuk, & Szalachowski, 2017). For example, previous work has described the destination as the weakest link (Bu et al., 2020).

It is also insufficient to merely enforce packet delivery along a specified path or verify which path a packet has taken. Path enforcement and path verification should be jointly adapted to accomplish path validation (PV). This strict requirement renders many routing and forwarding security applications unqualified for validating network paths. For example, the following applications may achieve secure routing or path enforcement but do not achieve path validation

(Bu et al., 2020):

- Secure routing: BGPsec, multipath routing and Secure Path Vector (SPV), Dysco, NIRA, RBF and many others
- Traceroute: DPM, PPM, Cherrypick, SPIE, NetSight
- Path verification or ‘secure traceroute’ (alone): such as Audit, RPVM, SPP
- Path enforcement or ‘secure source routing’ (alone): such as ARROW, HORNET, Onion routing, Platypus, Tor

In path validation, cryptographically computed path data is embedded within a packet header and PV applications must meet both path verification and enforcement capability criteria. As a result, PV measures have arisen in the literature and are discussed in subsequent sections, though there are very few that meet the criteria (Bu et al., 2020).

4.3 Anomaly detection (AD) for incident response

Security Operations Centres (SOCs) utilise monitoring and incident response applications such as Security Information Management (SIM) and Security Information and Event Management (SIEM) (Nabil, Soukainat, Lakbabi, & Ghizlane, 2017; Sekharan & Kandasamy, 2017). Similarly, several approaches to BGP incident detection, protection and response exist (Lad et al., 2006; Birge-Lee et al., 2021).

While an in-depth technical review of the underlying application methodologies is beyond the scope of this paper, we can categorise approaches into machine learning, reachability-based methods, statistical pattern recognition, time series analysis, validation approaches based on historical BGP data and novel ontological approaches using PageRank and Neighbour-Rank algorithms (Al-Musawi, 2018; Alkadi, Moustafa, Turnbull, & Choo, 2020).

In terms of security applications for BGP, previous research has shown that applications based on statistical pattern recognition, time-series and techniques utilising historical BGP data have

shown the more promise for real-time incident response application that can also identify the source cause and location (Al-Musawi, 2018). However, the ability for a BGP incident detection and response application to detect the attack in real-time, identify the source and, finally, differentiate between different types of attacks, remains elusive (Al-Musawi, Branch, & Armitage, 2016). Additionally, as with many areas of anomaly detection in cyber security, data ground truth can be elusive (Johnstone & Peacock, 2020). To some extent, the MANRS observatory platform does address anomaly detection, visibility and mitigation. The platform draws on a range of information sources to quickly identify Internet routing incidents and provide verifiable attribution as to their nature and origin.

5. MANRS AS A PRACTICAL IMPLEMENTATION FRAMEWORK

There has been very little discussion on the practical operationalisation of norms developed in the international cyber governance frameworks (e.g., UN OEWG and GGE). Here, via a semi-thematic analysis of the Cyber Norms incorporated by these cyber governance frameworks, viz. the use of MANRS as a practical implementation framework is posited. Table 1 illustrates if MANRS uses a category of Internet security control (as outlined in section 4), denoted as Yes (Y), No (N) or Partial (P), to address a UN Cyber Norm analysed below.

From this analysis we can see that the MANRS framework can address a number of norms via RSPG and ROV solutions. However, in PV and IDPR security application categories there was no evidence that MANRS currently utilises PV nor IDPR security applications, that would contribute to a comprehensive operationalisation of Cyber Norms. We leave any further discussion and exploration on operationalisation of these norms or other international law approaches, to future research opportunities.

Table 1: UN Cyber Norms and Internet routing security

	RSPG	ROV	PV	AD
Cyber Norm1	Y	Y	P	P
Cyber Norm2	Y	N	N	P
Cyber Norm3	Y	N	N	N
Cyber Norm4	Y	P	P	P
Cyber Norm5	N	N	N	N
Cyber Norm6	N	N	N	N
Cyber Norm7	Y	Y	P	P
Cyber Norm8	Y	Y	P	P
Cyber Norm9	N	N	N	N
Cyber Norm10	Y	Y	P	P
Cyber Norm11	P	P	P	P

6. BREAKING THE INTERNET

Malicious actors can manipulate the routing system to conduct cyber espionage, impose censorship, and execute disruption and sabotage operations (Demchak & Shavitt, 2018; Testart et al., 2019). The many businesses, transactions, devices, and global matters of state present on this shared resource every day can be at risk due to the inherent insecurity of the Internet’s inter-domain networking communication system (BGP) (Demchak & Shavitt, 2018). Similarly, the Internet forwarding-plane (the data plane) has shown to be vulnerable to attack and cyber-surveillance (Bu et al., 2020; Roberts & Plonka, 2020).

There have been a number of significant BGP incidents in recent years that include Internet traffic compromised and re-routed through state-owned telecommunications companies and ISPs (Demchak & Shavitt, 2018; Smith et al., 2020; Mitseva et al., 2018). BGP incidents and anomalies have been defined as damaging BGP activity that exist on a spectrum of impact (de Urbina Cazenave, Köşlük, & Ganiz, 2011; Cho et al., 2019; Al-Musawi, Branch, & Armitage, 2016). For example, BGP incidents can range from the relatively harmless (e.g., route-flapping) through to highly dangerous (e.g., BGP ‘hijacking’ and surgical interception); these can be driven by non-malicious or malicious intent

(Cho et al., 2019; Al-Musawi, Al-Saadi, Branch, & Armitage, 2016). Previous work has produced BGP anomaly taxonomy that encapsulate four categories: direct intended, direct unintended, indirect and link failure. Within each category, the authors further sub-classified BGP anomalies (Al-Musawi, Branch, & Armitage, 2016).

BGP hijacks and re-routing incidents can also range in granularity such as, same-prefix hijacking, sub-prefix hijack, AS path poisoning and increasingly surgical interception attacks (Cho et al., 2019; Birge-Lee et al., 2019). The same-prefix and sub-prefix hijacks can be used for interception whereby the malicious actor hijacks for the same prefix IP announced by the victim or a more specific prefix in IP (sub-prefix). For example, if a prefix was to be 10.0.0.0/16, a sub-prefix hijack attacker might announce the prefix 10.0.0.0/24 and BGP is based on a system of trust thus it will take the more direct (specific) route.

Another form of attack is the path poisoning attack approach that exploits the loop prevention mitigation in BGP; effectively and selectively inhibiting route propagation via the inclusion of a specific ASN in the path (Krupp & Rossow, 2021).

While a sub-prefix attack can effectively hijack (and intercept) BGP traffic, this can be detected by several measures due to the target importing the bogus route (Cho et al., 2019; Al-Musawi, Al-Saadi, et al., 2016). There exists stealthier and surgical interception attacks (Birge-Lee et al., 2019). For example, the BGP *communities* attribute can be used to sharpen and shape propagation of malicious routes.

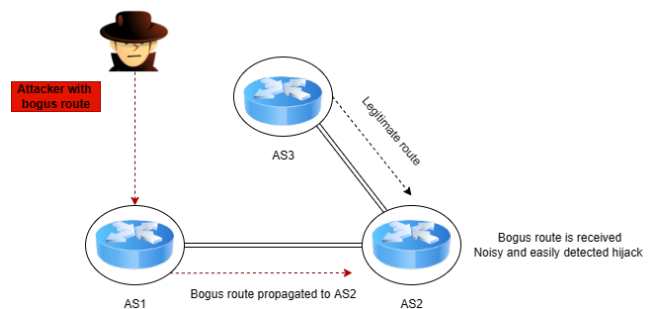


Figure 6: Noisy BGP hijack

Previous research has shown that up to 72 percent of domains are vulnerable to the most basic of BGP sub-prefix hijacks and up to 70 percent are vulnerable to same-prefix attacks (Birge-Lee et al., 2021). Research has also shown the ease of which bogus certificates could be obtained from the top five CAs and all were susceptible to standard BGP hijack attacks (Birge-Lee et al., 2018). Following these validated attacks, some CAs began implementing mitigation, though highly-targeted surgical BGP attacks by stealth remain a threat (Birge-Lee et al., 2019, 2018).

7. BGP INTERCEPTION ATTACKS BY STEALTH

BGP hijacks and re-routing incidents can range in granularity (e.g., same-prefix hijacking, sub-prefix hijack and AS path poisoning) (Cho et al., 2019; Birge-Lee et al., 2019). BGP is the default inter-domain routing protocol for the Internet and has been revised multiple times since the first Request for Comment (RFC) proposal issued in 1989 (Jain & Edgeworth, 2016; Loughheed & Rekhter, 1989, 1991). RFCs exist as an internet engineering and governance corpus (Braman, 2017). Several characteristics of BGP can be exploited to achieve hijacking and interception by stealth. We first provide a brief review of BGP before further describing surgical BGP interception attacks.

7.1 BGP anatomy and function

BGP is both a path-vector and incremental routing protocol (Bookham, 2014; Tomsho, 2012); it has also been described as a distance-vector variant (Huston & Armitage, 2006). Path attributes help determine a best-path routing decision and are found in a BGP message (Bookham, 2014). The four attribute categories are: well-known mandatory (e.g. the Origin and AS-PATH attributes), well-known discretionary (e.g. the LOCAL-PREF attribute), optional transitive (e.g. the AGGREGATOR attribute), and optional non-transitive (e.g. the MED attribute).

The task of BGP configuration is largely influenced by policies and AS relationships. BGP at-

tributes can define policies, and where no policy exists the minimum AS-PATH length is considered the optimal route. The interconnection of ASes are underpinned by three general relationship categories: customer-provider, peer-to-peer, and sibling-to-sibling. A detailed review of BGP configuration is beyond the scope of this paper; in summary - the policies enforce the relationships.

7.2 BGP community and traffic shaping

As a result of extant routing relationships and policies, upstream AS routing policy can be shaped by BGP communities when added to a BGP message. The community attributes (e.g., as defined in RFCs 1997, RFC 3765, RFC 7999) can be used to influence other AS announcement behavior and shape the propagation of bogus BGP messages; this can be used for surgical BGP hijack interception by stealth (Birge-Lee et al., 2019). This enables a fine-grained highly-targeted interception attack where other attacks are more visible (or ‘noisy’). We design an educational case study for such an attack in section 9.

In Figure 6 we can see that AS2 will hear the legitimate route from provider AS3, however it will also hear the (bogus) route from the AS1 peer; the LOCAL-PREF attribute may result in AS2 accepting the malicious route but it will thus result in a noisy attack. We can see in Figure 7 that an attack-by-stealth is achievable when the BGP community attributes are manipulated. These specific attacks have been previously described in the literature (Birge-Lee et al., 2019).

8. BGP EDUCATION: THE ELEPHANT IN THE ROOM

How cyber security education is to address the realities of scalable practices in some of the world’s largest companies have been previously considered in the literature (Caelli, 2020; Austin, 2020). Both educational institutions (e.g., Universities) and network/cyber security specific operator training institutions (e.g., Cisco, Juniper, CISSP) are destinations for students.

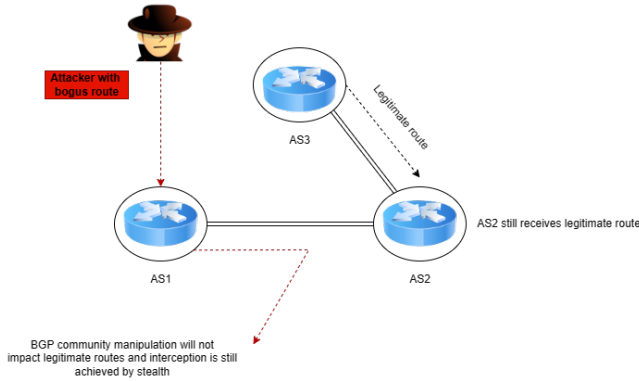


Figure 7: BGP hijack and interception by stealth

As was discussed in previous sections, the practical implementation and application of cyber security norms would have to involve Tier-1 networks, ISPs, IXPs, CDNs and ASes that represent the critical Internet infrastructure. This means that it will be the network operators employed within these organisations (and others) that form the frontline of practical implementation. Section 3 outlined categories of currently available cyber security techniques and applications for internet security engineering and cyber security practitioners. However, unless global cyber security curricula does address BGP security there will be a deficit in formally validating knowledge, skills and abilities (KSA) in BGP security. A cyber security body of knowledge and framework can influence education programs and students globally (Blair, Hall, & Sobiesk, 2020). Knowledge areas are an important element of these frameworks. Based on an approach previously outlined in the literature, though for a different purpose (Furnell & Bishop, 2020; Scott & Mason, 2022), we perform a preliminary review of some predominant Bodies of Knowledge (BoKs) and education frameworks for themes of ‘BGP’ and ‘BGP security’. We leave a systematic thematic review of cyber security educational curricula studies for future research. Similar to the approach taken in previous research (Furnell & Bishop, 2020; Scott & Mason, 2022), we chose to survey the following items:

- Cyber Security Body of Knowledge (CyBOK)

- Cyber Security Education Curriculum (CSEC)
- National Centers of Academic Excellence in Cyber security (NCAE-C) Cyber Defence Education Curricula (CAE-CD)

The CyBOK project approach to knowledge area development, drew inspiration from the Software Engineering Body of Knowledge (the SWEBOK)(Martin & Collier, 2020). Within the CSEC body of knowledge, there are eight knowledge areas that have previously been discussed in the literature (Shoemaker, Kohnke, & Sigler, 2019). The CAE-CD was also reviewed and contains some 69 units in total; the CAE-CD has three foundational units, five technical units, five non-technical units, and the remainder as option units (*CAE Documents Library – DoD Cyber Exchange*, 2020).

The CyBOK covers some aspects of BGP. For example, BGP hijacks are briefly discussed in Section 8, though it is proposed that the attacks are not worth the gain (Rashid, Chivers, Danezis, Lupu, & Martin, 2021, p.260), despite some attacks being achievable in less than a minute for a net gain of almost two million dollars (Cimpanu, 2022; Birge-Lee et al., 2021). BGP security is also discussed as a topic in the Network Layer Security section, though it only identifies BGPsec as a mitigation (Rashid et al., 2021, p.566). While BGPsec was proposed to address PV challenges, there are several more control categories and many more mitigations extant, which was specifically outlined in Section 4 of this paper.

The NSA’s CAE-CD has a knowledge area on BGP under the ‘Advanced Routing algorithms and protocols’ topic, in the section Advanced Network Technology and Protocols (ANT) (*CAE Documents Library – DoD Cyber Exchange*, 2020, p.33). This topic within the knowledge unit is one of nine (11%), and the knowledge unit itself is an optional knowledge unit and represents one unit out of 69 total units (1.45%).

We found no evidence the Cyber Security Education Curriculum (CSEC) body of knowledge addresses BGP or BGP security topics specifically.

Finally, a review of a major network education, skills and training provider shows evidence that BGP was subject matter as part of its most popular global networking certificate curricula and materials and covered BGP or BGP security topics until 2020 (specifically the external interdomain protocol as opposed to internal BGP). Since 2020, the content has largely been removed. We discuss some of the implications of this removal in section 10.

9. CASE STUDY: BGP INTERCEPTION ATTACK SIMULATION SCENARIO

The following case study and Capture the Flag (CTF) scenario design has been inspired by a previous CTF architecture produced for the popular Hack the Box education and training platform, where compromising FTP via a BGP hijack was the ultimate objective (Lemire, 2019). As previously outlined, a BGP hijack was recently used by malicious actors to steal almost two million dollars worth of cryptocurrency from a South Korean platform. This is a scenario design for an educational CTF Virtual Machine (VM) to simulate a similar stealthy and targeted BGP attack; in this scenario to ultimately manipulate domain control verification processes, rapidly acquire a certificate, and control DNS lookup processes for HTTP (or Email) verification.

Here we describe some proposed technical considerations and the overall steps of the CTF. We operationalise previous research on CA attacks to implement the attacks described into an educational resource architecture (Birge-Lee et al., 2021). It is our objective that educators and trainers might also be inspired to design and engineer similar CTF and VM architectures to better educate and train practitioners on BGP hijacking impacts.

The AS parties include AS1-R1 a fictitious small ISP (LittleISP) that owns the fictitious domain littleisp.com, AS2-R2 the server of littleisp.com, and AS3-R3 the fictitious CA (YoMama). The proposed Operating System architectures of the CTF VM and containers are

Ubuntu Linux 18.04 for the host OS and Ubuntu Linux 16.04 LXC for the containers. The web container that hosts the web application, is an initial point of compromise and AS1-R1, AS2-R2 and AS3-R3 are three containers running Quagga, simulating the three ASes. Additional containers for DNS and other CA operations can be implemented for more advanced simulations. In addition to BGP hijacking, other preliminary foothold attacks include dirbusting and command injections.



Figure 8: Overview of CTF steps

9.1 Introduction

Critical to many forms of encrypted communication are digital certificates. Public Key Infrastructure (PKI) facilitates the signing of certificates by third-party Certificate Authorities (CAs), such as Comodo, GoDaddy, Global-Sign, Let’s Encrypt and Symantec. Publicly trusted CA lists are retained in TLS clients and web browsers.

Many sensitive forms of communication (e.g., banking, financial, health) rely on such infrastructure. For example, in our CTF design the fictitious CA (YoMama) would be legitimately asked to sign a certificate; however the CA must validate that the client or domain owner (LittleISP) is actually the entity making the request. This is a process of domain control verification. However, this domain control verification process is vulnerable to attack, such as Man-in-the-Middle (MITM) operations, and can be spoofed via targeted BGP interception to obtain certificates.

9.2 Overview of attack steps

We escalate an attack from a web target (login page) to either a standard sub-prefix hijack (more detectable) or a very specific form of BGP hijack that is very difficult to detect, and ulti-

mately to the MITM on CAs—spoofing the domain verification process and obtaining a certificate from the CA (YoMama).

9.2.1 Initial compromise and port scan

Like many ethical (or unethical) hacking activities, the first step is reconnaissance using a port scanner. In this case study, we perform an nmap port scan that provides information on open ports for SSH and HTTP (i.e., ports 20 and 80).

9.2.2 Further enumeration

Via web enumeration the participant will eventually arrive at a web page. No default credentials nor SQL approaches will be successful at this stage. What appears to be error codes will be displayed. These are hints that are required in later steps.

9.2.3 Web server hunting

The next step is to use dirbusting, a technique for brute forcing directories and files on web servers (e.g., the GoBusting tool), to find potentially interesting artefacts (Antonelli, Cascella, Perrone, Romano, & Schiano, 2021). The participant will discover a number of different directories and files, some helpful and some not. For example, in this CTF exercise we seed a network diagram and a PDF containing an appendix listing error codes. The topology is a hint for later BGP hijacking and the error codes in the PDF match two that were previously found at the login web page. The participant will then discover the errors relate to an expired license and that the default ‘admin’ account uses the chassis serial number of the device as the password (the participant will need to obtain this in further steps).

9.2.4 SNMP reconnaissance and enumeration

Information such as device serial numbers can often be found on SNMP Management Information Bases (MIBs). The serial number (and admin password) of the device can be obtained via SNMP reconnaissance and enumeration and querying the box with the default public SNMP community string. The participant can then obtain a serial number (the password), obtaining

admin credentials to compromise the web app and login where they are presented with the dashboard of the fictitious victim LittleISP.

9.2.5 Dashboard analysis and command injection

A number of hints are placed in a series of ticketing system updates and conversations in the LittleISP dashboard. Such as one about a CA, Let’sCry(pt), having issued warnings about certificates being obtained by malicious actors and the need for ‘MultiVP’ responses. Another example includes a network engineer stating that “the CA YoMama domain verification is fine” and effectively ignores it. Another refers to “leak routes” from an upstream ISP. One of their important clients is having “serious problems” on their x.x.x.x/23 network.

As will be outlined in further steps, the participant will ultimately need to pursue why the /23 network is so important. Ultimately the participant will intercept HTTP traffic (or email traffic depending on the CA) for a MITM attack using BGP hijacks.

In the next steps, the participant can perform some command injections in the diagnostics tab of the dashboard. HTML response provides some base64 to be decoded and, once done, the participant decodes to plaintext ‘quagga’. The output will also show AS1-R1 is running the command due to it having an SSH connection with the web server on which it runs the command. A reverse shell can be obtained on AS1-R1 using netcat.

In preparing to escalate to a BGP hijack we note that BGP attacks are achievable both on the fictitious ISP and CA at this point (Birge-Lee et al., 2018). How a participant deploys their attack will be dependent on their knowledge and skill level.

9.2.6 BGP hijack and interception attack

We might consider for a moment that a standard sub-prefix BGP attack is possible at this point. One of the reasons such an attack is easily detectable, as opposed to a surgical BGP hijack, is that should we simply inject a more specific route for the target, to intercept and cap-

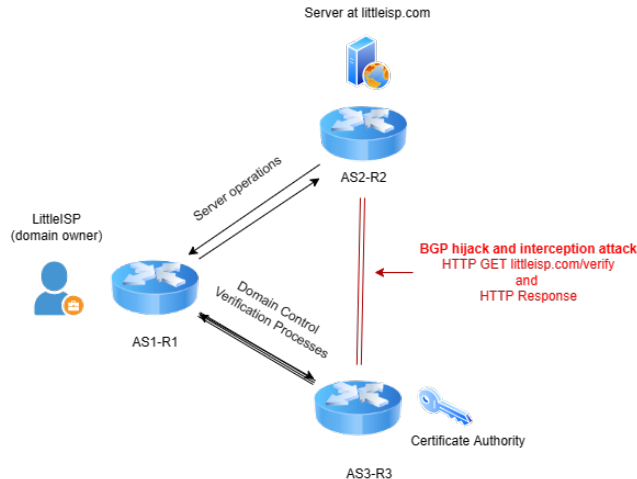


Figure 9: BGP hijack and interception

ture traffic, unless there is a measure deployed to prevent traffic being intercepted and then forwarded through to destination, such an attack is easily detected. As previously described, the exploitation of the BGP communities attributes (e.g., RFC 1997, RFC 3765, RFC 7999) allow an attacker to prevent such an outcome yet intercept by stealth (Birge-Lee et al., 2019).

At this point a participant has several options for the BGP attack on the /23 network (e.g., sub-prefix hijack using /24 or a surgical BGP attack exploiting BGP communities). Consider an approach where the attacker issues a signing request for LittleISP’s digital certificate to the CA, whereby the CA processes verification steps (e.g., via HTTP GET request) then proceed. The BGP insertion point for the attack is relatively trivial and interception achievable at this point – the CA’s request is redirected to the attacker who is now capable of responding to the HTTP request for the domain control verification process (Figure 9).

9.2.7 Advanced

It is also possible to move beyond BGP interception and domain verification spoofing to target LittleISP’s DNS server. Configuration of an adversarial server for these purposes is relatively trivial. Traffic to the LittleISP DNS server can be captured, the adversarial server provides the bogus response, the DNS lookup verification pro-

cess is executed by the CA and the adversary is responding. Ultimately a HTTP request is sent to the malicious actor’s adversarial server.

10. DISCUSSION AND CONCLUSION

The Internet is a globally-scaled complex system, therefore it is unsurprising that global approaches to address Internet routing security challenges have been conducted and the attendant security challenges are complex.

The multi-dimensional nature of Internet routing and protocol infrastructure requires robust solutions for security practitioners; origin and path validation in addition to incident detection and response are all active areas of research for these reasons. The slower a defense application or mitigation identifies a BGP attack, the more effective and damaging the attack can be. Further research on Internet protocol insecurity and attack detection is required to improve tools for SOC analysts and DFIR professionals.

However, it is of concern that BGP security topics are either minimally addressed or non-existent in some predominant networking and security BoKs, frameworks and curricula. We found that one major network training entity removed interdomain BGP security as a topic. At least one major curriculum document in this cyber security education corpus also states that BGP attacks are not worth the exercise, yet attacks have been shown achievable in less than a minute for a net gain of almost two million dollars (Cimpanu, 2022; Birge-Lee et al., 2021).

As a practical example for including BGP security in cyber security education curricula we have presented one case study and CTF scenario to simulate a highly targeted BGP interception attack that obtains a certificate for a victim’s domain and then decrypts sensitive traffic. This CTF design is one contribution and exemplar for practical cyber security education, advanced Internet emulations for education also exist (Du, 2022). We plan to release an operational version of the CTF via a GitHub repository in the future. It is our objective that educators and trainers might also be inspired to design and en-

gineer similar architectures to better educate and train practitioners on the impact of BGP attacks, while cyber security curricula designers might be motivated to address the important topic of BGP security.

11. ACKNOWLEDGMENTS

The work was supported by the Cyber Security Research Centre Limited whose activities are partially funded by the Australian Government's Cooperative Research Centres Programme.

REFERENCES

- Alderson, D. L., Doyle, J. C., & Willinger, W. (2019, November). Lessons from "a First-Principles Approach to Understanding the Internet's Router-Level Topology". *SIGCOMM Comput. Commun. Rev.*, 49(5), 96–103. Retrieved from <https://doi.org/10.1145/3371934.3371964> (Place: New York, NY, USA Publisher: Association for Computing Machinery) doi: 10.1145/3371934.3371964
- Alkadi, O. S., Moustafa, N., Turnbull, B., & Choo, K.-K. R. (2020). An Ontological Graph Identification Method for Improving Localization of IP Prefix Hijacking in Network Systems. *IEEE Transactions on Information Forensics and Security*, 15, 1164–1174. (Conference Name: IEEE Transactions on Information Forensics and Security) doi: 10.1109/TIFS.2019.2936975
- Al-Musawi, B. (2018). *Detecting BGP Anomalies Using Recurrence Quantification Analysis* (Unpublished doctoral dissertation). Ph. D. dissertation, Swinburne University of Technology.
- Al-Musawi, B., Al-Saadi, R., Branch, P., & Armitage, G. (2016). BGP replay tool (BRT) v0.1. *I4T Research Lab, Swinburne University of Technology, Melbourne, Australia, Tech. Rep. A, 170606*, 06.
- Al-Musawi, B., Branch, P., & Armitage, G. (2016). BGP anomaly detection techniques: A survey. *IEEE Communications Surveys & Tutorials*, 19(1), 377–396.
- Antonelli, D., Cascella, R., Perrone, G., Romano, S. P., & Schiano, A. (2021). Leveraging ai to optimize website structure discovery during penetration testing. *arXiv preprint arXiv:2101.07223*.
- Austin, G. (2020). *Cyber Security Education: Principles and Policies*. UK: Routledge. (Google-Books-ID: LWHwDwAAQBAJ)
- Ball, J. (2020). *The Tangled Web We Weave: Inside the Shadow System That Shapes the Internet*. Melville House Publishing.
- Barrera, D., Chuat, L., Perrig, A., Reischuk, R. M., & Szalachowski, P. (2017, May). The SCION internet architecture. *Commun. ACM*, 60(6), 56–65. Retrieved 2022-02-10, from <https://dl.acm.org/doi/10.1145/3085591> doi: 10.1145/3085591
- Birge-Lee, H., Sun, Y., Edmundson, A., Rexford, J., & Mittal, P. (2018, August). Bambooing certificate authorities with BGP. In *Proceedings of the 27th USENIX Conference on Security Symposium* (pp. 833–849). USA: USENIX Association.
- Birge-Lee, H., Wang, L., McCarney, D., Shoemaker, R., Rexford, J., & Mittal, P. (2021, August). Experiences deploying Multi-Vantage-Point domain validation at let's encrypt. In *30th usenix security symposium (usenix security 21)* (pp. 4311–4327). USENIX Association. Retrieved from <https://www.usenix.org/conference/usenixsecurity21/presentation/birge-lee>
- Birge-Lee, H., Wang, L., Rexford, J., & Mittal, P. (2019, November). SICO: Surgical Interception Attacks by Manipulating BGP Communities. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 431–448). New York, NY, USA: Association for Computing Machinery. Retrieved 2020-12-08, from <https://doi.org/10.1145/3319535.3363197> doi: 10.1145/3319535.3363197
- Blair, J. R. S., Hall, A. O., & Sobiesk, E. (2020). Holistic cyber education. In *Cyber Security Education* (pp. 160–172). UK: Routledge. (Num Pages: 13)

- Boitmanis, K., Brandes, U., & Pich, C. (2008). Visualizing Internet Evolution on the Autonomous Systems Level. In S.-H. Hong, T. Nishizeki, & W. Quan (Eds.), *Graph Drawing* (pp. 365–376). Berlin, Heidelberg: Springer. doi: 10.1007/978-3-540-77537-9_36
- Bookham, C. (2014). *Versatile Routing and Services with BGP: Understanding and Implementing BGP in SR-OS*. John Wiley & Sons.
- Broeders, D., & Cristiano, F. (2020). Cyber Norms and the United Nations: Between Strategic Ambiguity and Rules of the Road. *SSRN Journal*. Retrieved 2021-07-12, from <https://www.ssrn.com/abstract=3819171> doi: 10.2139/ssrn.3819171
- Bu, K., Laird, A., Yang, Y., Cheng, L., Luo, J., Li, Y., & Ren, K. (2020, September). Unveiling the Mystery of Internet Packet Forwarding: A Survey of Network Path Validation. *ACM Comput. Surv.*, 53(5), 104:1–104:34. Retrieved 2021-02-15, from <https://doi.org/10.1145/3409796> doi: 10.1145/3409796
- Bu, K., Yang, Y., Laird, A., Luo, J., Li, Y., & Ren, K. (2018). *What's (not) validating network paths: A survey*.
- Buchanan, B. (2020). *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics*. United States: Harvard University Press. (Google-Books-ID: NE3SDwAAQBAJ)
- CAE Documents Library – DoD Cyber Exchange. (2020). Retrieved 2022-03-02, from <https://public.cyber.mil/ncae-c/documents-library/>
- Caelli, W. J. (2020). History and philosophy of cyber security education. In *Cyber Security Education* (pp. 8–28). UK: Routledge. (Num Pages: 21)
- Cerf, V. G., & Kahn, R. E. (2005, April). A protocol for packet network intercommunication. *ACM SIGCOMM Computer Communication Review*, 35(2), 71–82. Retrieved 2020-12-08, from <https://doi.org/10.1145/1064413.1064423> doi: 10.1145/1064413.1064423
- Cho, S., Fontugne, R., Cho, K., Dainotti, A., & Gill, P. (2019). BGP hijacking classification. In (pp. 25–32). IEEE.
- Chung, T., Aben, E., Bruijnzeels, T., Chandrasekaran, B., Choffnes, D., Levin, D., ... Sullivan, N. (2019, October). RPKI is Coming of Age: A Longitudinal Study of RPKI Deployment and Invalid Route Origins. In *Proceedings of the Internet Measurement Conference* (pp. 406–419). Amsterdam Netherlands: ACM. Retrieved 2022-02-10, from <https://dl.acm.org/doi/10.1145/3355369.3355596> doi: 10.1145/3355369.3355596
- Cimpanu, C. (2022, February). *KlaySwap crypto users lose funds after BGP hijack* [Threat Intelligence]. Retrieved 2022-03-02, from <https://therecord.media/klayswap-crypto-users-lose-funds-after-bgp-hijack/>
- Demchak, C. C., & Shavitt, Y. (2018). China's Maxim-Leave No Access Point Unexploited: The Hidden Story of China Telecom's BGP Hijacking. *Military Cyber Affairs*, 3(1), 7.
- de Urbina Cazenave, I. O., Köşlük, E., & Ganiz, M. C. (2011). An anomaly detection framework for BGP. In (pp. 107–111). IEEE.
- Du, W. (2022). SEED Internet Emulator: An Open-Source Tool for Network and Cybersecurity Courses. In *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education V. 2* (pp. 1180–1180). Providence RI USA: ACM. Retrieved 2022-07-19, from <https://dl.acm.org/doi/10.1145/3478432.3499260> doi: 10.1145/3478432.3499260
- Feakin, T., & Weaver, J. (2020). *Cyber diplomacy: An Australian perspective* (1st ed.). New York: Routledge, Taylor & Francis Group.
- Freedman, D., Foust, B., Greene, B., Maddison, B., Robachevsky, A., Snijders, J., & Steffann, S. (2018). *Mutually Agreed Norms for Routing Security (MANRS) Implementation Guide* (Tech. Rep.). RIPE. Retrieved from

- <https://www.ripe.net/publications/docs/ripe-706> (Publisher: RIPE Documents ripe-706. RIPE. <https://www.ripe.net/publications/docs/ripe-706>)
- Furnell, S., & Bishop, M. (2020, February). Addressing cyber security skills: the spectrum, not the silo. *Computer Fraud & Security*, 2020(2), 6–11. Retrieved 2021-04-14, from <https://www.sciencedirect.com/science/article/pii/S1361372320300178> doi: 10.1016/S1361-3723(20)30017-8
- Gisel, L., Rodenhäuser, T., & Dörmann, K. (2020). Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. *International Review of the Red Cross*, 101(112), 1–48. Retrieved from <https://international-review.icrc.org/articles/twenty-years-ihl-effects-of-cyber-operations-during-armed-conflicts-913> (Edition: 2020/10/26 Publisher: Cambridge University Press) doi: 10.1017/S1816383120000387
- Gold, J. (2021, March 18). *Unexpectedly, All UN Countries Agreed on a Cybersecurity Report. So What?* Retrieved 2021-08-26, from <https://www.cfr.org/blog/unexpectedly-all-un-countries-agreed-cybersecurity-report-so-what>
- Greenberg, A. (2018, August). *The untold story of NotPetya, the most devastating cyber-attack in history*. New York, NY, USA. Retrieved from <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> (Publisher: Wired)
- Hesselman, C., Grosso, P., Holz, R., Kuipers, F., Xue, J. H., Jonker, M., . . . de Laat, C. (2020, October). A Responsible Internet to Increase Trust in the Digital World. *J Netw Syst Manage*, 28(4), 882–922. Retrieved 2021-07-12, from <http://link.springer.com/10.1007/s10922-020-09564-7> doi: 10.1007/s10922-020-09564-7
- Huston, G., & Armitage, G. J. (2006). Projecting future ipv4 router requirements from trends in dynamic bgp behaviour. In *Australian Telecommunication Networks and Applications Conference (ATNAC)*.
- Jain, V., & Edgeworth, B. (2016). *Troubleshooting BGP: A Practical Guide to Understanding and Troubleshooting BGP*. Cisco Press. (Google-Books-ID: LPLB-DQAAQBAJ)
- Johnstone, M., & Peacock, M. (2020). Seven Pitfalls of Using Data Science in Cybersecurity. In L. F. Sikos & K.-K. R. Choo (Eds.), *Data Science in Cybersecurity and Cyberthreat Intelligence* (Vol. 177, pp. 115–129). Cham: Springer International Publishing. Retrieved 2022-06-21, from http://link.springer.com/10.1007/978-3-030-38788-4_6 (Series Title: Intelligent Systems Reference Library) doi: 10.1007/978-3-030-38788-4_6
- Kim, T. H.-J., Basescu, C., Jia, L., Lee, S. B., Hu, Y.-C., & Perrig, A. (2014, August). Lightweight source authentication and path validation. In *Proceedings of the 2014 ACM conference on SIGCOMM* (pp. 271–282). Chicago Illinois USA: ACM. Retrieved 2022-02-10, from <https://dl.acm.org/doi/10.1145/2619239.2626323> doi: 10.1145/2619239.2626323
- Kirkpatrick, K. (2021, August). Fixing the internet. *Commun. ACM*, 64(8), 16–17. Retrieved 2021-08-30, from <https://dl.acm.org/doi/10.1145/3469287> doi: 10.1145/3469287
- Krupp, J., & Rossow, C. (2021). Bgpeek-a-boo: Active bgp-based traceback for amplification ddos attacks. In *2021 ieee european symposium on security and privacy (euros p)* (p. 423-439). doi: 10.1109/EuroSP51992.2021.00036
- Lad, M., Massey, D., Pei, D., Wu, Y., Zhang, B., & Zhang, L. (2006, July). PHAS: A prefix hijack alert system. In *15th usenix security symposium (usenix security 06)*. Vancouver, B.C. Canada: USENIX Association. Retrieved from <https://www.usenix.org/conference/>

- 15th-usenix-security-symposium/
phas-prefix-hijack-alert-system
- Lad, M., Zhao, X., Zhang, B., Massey, D., & Zhang, L. (2003). Analysis of BGP update surge during slammer worm attack. In (pp. 66–79). Springer.
- Legner, M., Klenze, T., Wyss, M., Sprenger, C., & Perrig, A. (2020). {EPIC}: Every packet is checked in the data plane of a path-aware internet. In *29th {USENIX} security symposium ({USENIX} security 20)* (pp. 541–558).
- Lemire, S. (2019, March). *Carrier - Hack The Box*. Retrieved 2022-03-02, from <https://snowscan.io/htb-writeup-carrier/>
- Lougheed, K., & Rekhter, Y. (1989). *RFC1105: Border Gateway Protocol (BGP)*. RFC Editor.
- Lougheed, K., & Rekhter, Y. (1991). *A border gateway protocol 3 (bgp-3)* (Tech. Rep.). RFC 1267, Cisco Systems, TJ Watson Research Center, IBM Corp.
- MANRS Observatory*. (n.d.). Retrieved 2021-08-30, from <https://observatory.manrs.org/>
- Martin, A., & Collier, J. (2020). Beyond awareness: Reflections on meeting the interdisciplinary cyber skills demand. In *Cyber Security Education* (pp. 55–73). UK: Routledge. (Num Pages: 19)
- Maurer, T. (2020, August). A Dose of Realism: The Contestation and Politics of Cyber Norms. *Hague J Rule Law*, 12(2), 283–305. Retrieved 2021-07-12, from <http://link.springer.com/10.1007/s40803-019-00129-8> doi: 10.1007/s40803-019-00129-8
- Meyer, P. (2020). Norms of Responsible State Behaviour in Cyberspace. In M. Christen, B. Gordijn, & M. Loi (Eds.), *The Ethics of Cybersecurity* (Vol. 21, pp. 347–360). Cham: Springer International Publishing. (Series Title: The International Library of Ethics, Law and Technology)
- Mitseva, A., Panchenko, A., & Engel, T. (2018). The state of affairs in BGP security: A survey of attacks and defenses. *Computer Communications*, 124, 45 – 60. Retrieved from <http://www.sciencedirect.com/science/article/pii/S014036641731068X> doi: <https://doi.org/10.1016/j.comcom.2018.04.013>
- Moriano, P., Hill, R., & Camp, L. J. (2019). Using Bursty Announcements for Early Detection of BGP Routing Anomalies. *arXiv preprint arXiv:1905.05835*.
- Motamedi, R., Yeganeh, B., Chandrasekaran, B., Rejaie, R., Maggs, B. M., & Willinger, W. (2019, October). On Mapping the Interconnections in Today’s Internet. *IEEE/ACM Transactions on Networking*, 27(5), 2056–2070. (Conference Name: IEEE/ACM Transactions on Networking) doi: 10.1109/TNET.2019.2940369
- Nabil, M., Soukainat, S., Lakbabi, A., & Ghizlane, O. (2017, May). SIEM selection criteria for an efficient contextual security. In *2017 International Symposium on Networks, Computers and Communications (ISNCC)* (pp. 1–6). Marrakech, Morocco: IEEE. Retrieved 2022-02-15, from <http://ieeexplore.ieee.org/document/8072035/> doi: 10.1109/ISNCC.2017.8072035
- Rashid, A., Chivers, H., Danezis, G., Lupu, E., & Martin, A. (2021, March). *The Cyber Security Body of Knowledge* (Tech. Rep. No. 1.1.0). UK: The National Cyber Security Centre. Retrieved from <https://www.cybok.org/media/downloads>
- Reuter, A., Bush, R., Cunha, I., Katz-Bassett, E., Schmidt, T. C., & Wählisch, M. (2018). Towards a rigorous methodology for measuring adoption of rpki route validation and filtering. *ACM SIGCOMM Computer Communication Review*, 48(1), 19–27.
- Roberts, L. M., & Plonka, D. (2020, June). Watching the Watchers: Nonce-based Inverse Surveillance to Remotely Detect Monitoring. *arXiv:2005.07641 [cs]*. Retrieved 2021-02-15, from <http://arxiv.org/abs/2005.07641> (arXiv: 2005.07641)
- Rodday, N., Ítalo S. Cunha, Bush, R., Katz-Bassett, E., Rodosek, G. D., Schmidt, T. C., & Wählisch, M. (2021). Re-

- visiting rpki route origin validation on the data plane. In V. Bajpai, H. Hadjadi, & O. Hohlfeld (Eds.), *5th network traffic measurement and analysis conference, tma 2021, virtual event, september 14-15, 2021*. IFIP. Retrieved from <http://dl.ifip.org/db/conf/tma/tma2021/tma2021-paper11.pdf>
- Roughan, M., Willinger, W., Maennel, O., Perouli, D., & Bush, R. (2011, October). 10 Lessons from 10 Years of Measuring and Modeling the Internet's Autonomous Systems. *IEEE Journal on Selected Areas in Communications*, 29(9), 1810–1821. doi: 10.1109/JSAC.2011.111006
- Scott, B., & Mason, R. (2022). Cyber as a Second Language? A Challenge to Cybersecurity Education. *CISSE*, 9(1), 6. Retrieved 2022-03-30, from <https://cisse.info/journal/index.php/cisse/article/view/137> doi: 10.53735/cisse.v9i1.137
- Sekharan, S. S., & Kandasamy, K. (2017, March). Profiling SIEM tools and correlation engines for security analytics. In *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)* (pp. 717–721). Chennai: IEEE. Retrieved 2022-02-15, from <http://ieeexplore.ieee.org/document/8299855/> doi: 10.1109/WiSPNET.2017.8299855
- Shoemaker, D., Kohnke, A., & Sigler, K. (2019, February). What the profession of cybersecurity needs to know and do. *null*, 59(2), 6–18. Retrieved from <https://doi.org/10.1080/07366981.2019.1565106> (Publisher: Taylor & Francis) doi: 10.1080/07366981.2019.1565106
- Smith, J. M., Birkeland, K., McDaniel, T., & Schuchard, M. (2020). Withdrawing the BGP Re-Routing Curtain: Understanding the Security Impact of BGP Poisoning through Real-World Measurements. In *Proceedings 2020 Network and Distributed System Security Symposium*. San Diego, CA: Internet Society. Retrieved 2020-12-08, from <https://www.ndss-symposium.org/wp-content/uploads/2020/02/24240.pdf> doi: 10.14722/ndss.2020.24240
- Srinivasan, C. (2017, November). Hobby hackers to billion-dollar industry: the evolution of ransomware. *Computer Fraud & Security*, 2017(11), 7–9. Retrieved from <http://www.sciencedirect.com/science/article/pii/S1361372317300817> doi: 10.1016/S1361-3723(17)30081-7
- Testart, C., & Clark, D. D. (2020). A Data-Driven Approach to Understanding the State of Internet Routing Security. *SSRN Journal*. Retrieved 2021-07-12, from <https://www.ssrn.com/abstract=3750155> doi: 10.2139/ssrn.3750155
- Testart, C., Richter, P., King, A., Dainotti, A., & Clark, D. (2019, October). Profiling BGP Serial Hijackers: Capturing Persistent Misbehavior in the Global Routing Table. In *Proceedings of the Internet Measurement Conference* (pp. 420–434). Amsterdam Netherlands: ACM. Retrieved 2021-07-12, from <https://dl.acm.org/doi/10.1145/3355369.3355581> doi: 10.1145/3355369.3355581
- Testart, C., Richter, P., King, A., Dainotti, A., & Clark, D. (2020). To Filter or Not to Filter: Measuring the Benefits of Registering in the RPKI Today. In A. Sperotto, A. Dainotti, & B. Stiller (Eds.), *Passive and Active Measurement* (pp. 71–87). Cham: Springer International Publishing.
- Tomsho, G. (2012). *Guide to networking essentials*. Cengage Learning.
- UN Cyber Norms. (2021, November 18). Retrieved 2021-08-24, from <https://www.aspi.org.au/cybernorms/downloads>
- UN GGE and OEWG. (2021, January 7). Retrieved 2021-08-26, from <https://dig.watch/processes/un-gge>