REFERENCES

Advanced Cyber Security Center (ACSC). (2019). Retrieved from https://www.massinsight.com/about-acsc/

Amante, S., Carpenter, B., Jiang, S., & Rajahalme, J. (2011, November). *IPv6 flow label specification*. RFC 6437. RFC Editor.

Ansible. (2019). Retrieved from https://www.redhat.com/en/technologies/management/ansible

Apple. (Ed.). (2016). *Apple Code Signing*. Retrieved from https://developer.apple.com/library/archive/documentation/Security/Conceptual/CodeSigningGuide/Introduction/Introduction.html

APWG. (2020, February). Phishing Activity Trends Report: Unifying the Global Response to Cybercrime. 4th Quarter 2019. Retrieved from https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf

Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005a, March). *DNS security introduction and requirements*. RFC 4033. RFC Editor.

Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005b, March). *Protocol modifications for the DNS security extensions*. RFC 4035. RFC Editor.

Arends, R., Austein, R., Larson, M., Massey, D., & Rose, S. (2005c). *Resource records for the DNS security extensions*. RFC 4034. RFC Editor.

Balfanz, D., Czeskis, A., Hodges, J., Jones, J. C., Jones, M. B., Kumar, A., ... Lundberg, E. (2019, March). Web authentication: An API for accessing public key credentials level 1. Retrieved from https://www.w3.org/TR/webauthn/

Barnes, R., Hoffman-Andrews, J., McCarney, D., & Kasten, J. (2019, March). *Automatic certificate management environment (ACME)*. RFC 8555. RFC Editor.

Bellovin, S., & Merritt, M. (1992). Encrypted key exchange: Password-based protocols secure against dictionary attacks. In IEEE Computer Society Symposium on Research in Security and Privacy, Oakland, California. doi:10.1109/RISP.1992213269

Bierman, A., Bjorklund, M., & Watsen, K. (2017, January). *RESTCONF protocol*. RFC 8040. RFC Editor.

Bittau, A., Giffin, D., Handley, M., Mazieres, D., Slack, Q., & Smith, E. (2019, May). *Cryptographic protection of TCP streams (tcpcrypt)*. RFC 8548. RFC Editor.

Bjorklund, M. (2016, August). *The YANG 1.1 data modeling language*. RFC 7950. RFC Editor.

Boyens, J., Paulsen, C., Moorthy, R., & Bartol, N. (2015, April). Supply chain risk management practices for federal information systems and organizations. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-161/final

Center for Internet Security. (Ed.). (2020). CIS critical security controls. Retrieved from https://www.cisecurity.org/controls/

Clark, D. D., Wroclawski, J., Sollins, K. R., & Braden, R. (2005, June). Tussle in cyberspace: Defining tomorrow's

internet. *Journal IEEE/ACM transactions on networking (TON)*, *13*(3), 462–475.

Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., & Polk, W. (2008, May). *Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile*. RFC 5280. RFC Editor.

Cox, T., & White, C. (2019). OASIS key management interoperability protocol (KMIP) TC. Ed. by OASIS. Retrieved from https://www.oasis-open.org/committees/kmip/

Crocker, D., Hansen, T., & Kucherawy, M. (2011, September). *DomainKeys identified mail (DKIM) signatures*. RFC 6376. RFC Editor.

CRUX Now. (Ed.). (2018). *China to regulate online religious activity among crackdown*. Retrieved from https://cruxnow.com/church-in-asia-oceania/2018/09/11/china-toregulate-online-religious-activity-amid-crackdown/

Curry. (2019, June). Indicators of behavior: The new telemetry to find advanced cyber attackers. Retrieved from https://www.forbes.com/sites/samcurry/2019/06/27/indicators-of-behavior-the-new-telemetry-to-find-advanced-cyberattackers/#7a769eb3193e

Deering, S., & Hinden, R. (2017, July). Internet protocol, version 6 (IPv6) specification. STD 86. RFC Editor.

DELL Technologies. (2019). *DELL unified workspace*. Retrieved from https://www.dellemc.com/en-us/unified-workspace/index.htm

Dickinson, S., Gillmor, D., & Reddy, T. (2018, May). *Usage profiles for DNS over TLS and DNS over DTLS*. RFC 8310. RFC Editor.

DMTF. (Ed.). (2020). *Common information model*. Retrieved from https://www.dmtf.org/standards/cim

Dukhovni, V., & Hardaker, W. (2015, October). *The DNS-based authentication of named entities (DANE) protocol: Updates and operational guidance*. RFC 7671. RFC Editor.

Dukhovni, V. (2014, December). *Opportunistic security: Some protection most of the time*. RFC 7435. RFC Editor.

Duo. (Ed.). (2019). *Cisco duo*. Retrieved from https://duo.com/

Elkins, N., Hamilton, R., & Ackermann, M. (2017, September). *IPv6 Performance and diagnostic metrics (PDM) destination option*. RFC 8250. RFC Editor.

Enns, R., Bjorklund, M., Schoenwaelder, J., & Bierman, A. (2011, June). *Network configuration protocol (NETCONF)*. RFC 6241. RFC Editor.

Farrell, S., & Tschofenig, H. (2014, May). Pervasive monitoring is an attack. RFC 7258. RFC Editor.

FIDO Alliance. (2019). Retrieved from https://fidoalliance.org/

Field, J., Banghart, S., & Waltermire, D. (2018, Febuary). *Resource-oriented lightweight information exchange (ROLIE)*. RFC 8322. RFC Editor.

Friel, O., Barnes, R., Shekh-Yusef, R., & Richardson, M. (2020, January). *ACME integrations*. RFC. RFC Editor. Retrieved from https://datatracker.ietf.org/doc/draft-ietf-acme-integrations/?include_text=1

General Dynamics. (Ed.). (2016). *About seL4*. Retrieved from https://sel4.systems/About/seL4/

Gidda, M. (2013). Edward Snowden and the NSA files – timeline. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/jun/23/edward-snowden-nsafiles-timeline

Gilder, G. (1992, December 7). The coming of the fibersphere. *Forbes ASAP*.

Gilder, G. (2018). *Life after Google: The fall of big data and the rise of the blockchain economy*. Washington, DC: Gateway Editions.. ISBN: 978-1621575764.

Gilman, E., & Barth, D. (2017). *Zero trust networks: Building secure systems in untrusted networks* (1st ed.). Sebastopol, CA: O'Reilly. ISBN: 978-1-491-96219-0.

Gont, F., Linkova, J., Chown, T., & Liu, W. (2016, June). Observations on the dropping of packets with IPv6 extension headers in the real world. RFC 7872. RFC Editor.

Google. (Ed.). (2019a). *Project zero*. Retrieved from https://googleprojectzero.blogspot.com/

Google. (Ed.). (2019b). *Safe browsing*. Retrieved from https://safebrowsing.google.com/

Google. (Ed.). (2019c). *TLS statistics-Google transparency report*. Retrieved from https://transparencyreport.google.com/https

Grassi, P., Fenton, J., Newton, E., Perner, R., Regenscheid, A., Burr, W. . . . Theofanos, M. (2017a, June). Authentication and lifecycle management. doi:10.6028/NIST.SP.800-63b

Grassi, P., Fenton, J., Lefkovitz, N., Danker, J., Choong, Y., Greene, K. . . . Theofanos, M. (2017b, June). Enrollment and identity proofing. doi:10.6028/NIST.SP.800-63a

Grassi, P., Richer, J., Squire, S., Fenton, J., Nadeau, E., Lefkovitz, N. . . . Theofanos, M. (2017c, June). Federation and assertions. doi:10. 6028/NIST.SP.800-63c

Grawrock, D., Wooten, D., & Goldman, K. (2016, September). *Trusted platform module library specification*. Committee draft family 2.0, level 00, revision 01.38. Trusted Computing Group.

Gross, J., Ganga, I., & Sridhar, T. (2019). *Geneve: Generic network virtualization encapsulation*. RFC. RFC Editor.

Retrieved from https://datatracker.ietf.org/doc/draft-ietfnvo3-geneve/

Hack the pentagon. (2019). Retrieved from https://www.hackerone.com/resources/hack-thepentagon

Halpern, J., & Pignataro, C. (2015, October). *Service function chaining (SFC) architecture*. RFC 7665. RFC Editor.

Hardt, D. (2012, October). *The OAuth 2.0 authorization framework*. RFC 6749. RFC Editor.

Herrera, E. (2016, June). Informed outsourcing. Retrieved from https://www.cio.com/article/3080095/cloud-delivers-on-outsourcings-promisebut-resultsmay-vary.html

HITRUST. (Ed.). (2020). *HITRUST security control framework*. Retrieved from https://hitrustalliance.net/

Hoffman, P., & McManus, P. (2018, October). *DNS Queries over HTTPS (DoH)*. RFC 8484. RFC Editor.

Hoffman, P., Sullivan, A., & Fujiwara, K. (2019). *DNS Terminology*. RFC8499. RFC Editor. IETF. Retrieved from https://tools.ietf.org/html/rfc8499

Housely, R., & Polk, T. (2001). *Planning for PKI: Best practices guide for deploying public key infrastructure* (1st ed.). New York, NY: Wiley Computer Publishing.

Hu, Z., Zhu, L., Heidemann, J., Mankin, A., Wessels, D., & Hoffman (2016, May). *Specification for DNS over transport layer security (TLS)*. RFC 7858. RFC Editor.

Information Technology Laboratory Computer Security Division. (2006, March). Minimum security requirements for federal information and information systems. Retrieved from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

Intel, Microsoft research and duality technologies convene AI community for privacy standards. (2019a, August). Retrieved from https://newsroom.intel.com/news/intel-microsoft-research-duality-technologies-convene-ai-communityprivacy-standards/#gs.urvz7w

Internet Architecture Board and Internet Engineering Steering Group. (2000, May). *IETF Policy on wiretapping*. RFC 2804. RFC Editor.

Internet Engineering Task Force. (Ed.). (2020a). *Security automation and continuous monitoring (SACM)*. Retrieved from https://datatracker.ietf.org/wg/sacm/about/

Internet Engineering Task Force. (Ed.). (2020b). *Trusted execution environment provisioning*. Retrieved from https://datatracker.ietf.org/wg/teep/about/

Internet Engineering Task Force. (Ed.). (2020c). *Authentication and authorization for constrained environments (ACE)*. Retrieved from https://datatracker.ietf.org/wg/ace/about/

Internet Engineering Task Force. (Ed.). (2020d). *IP security maintenance and extensions (ipsecme)*. Retrieved from *https://datatracker.ietf.org/wg/ipsecme/about/*

Internet Engineering Task Force. (Ed.). (2020e). *QUIC*. Retrieved from https://datatracker.ietf.org/wg/quic/about/

Internet Engineering Task Force. (Ed.). (2020f). *Remote ATtestation procedureS (RATS)*. Retrieved from https://datatracker.ietf.org/wg/rats/about/

Internet Engineering Task Force. (Ed.). (2020g). *TCP increased security (tcpinc)*. Retrieved from https://datatracker.ietf.org/wg/tcpinc/about/

Internet Engineering Task Force. (2020h). *Automated certificate management environment (ACME)*. Retrieved from https://datatracker.ietf.org/wg/acme/about/

Internet Research Task Force. (Ed.). (2019). *CFRG PAKE selection information and repository*. Retrieved from https://github.com/cfrg/pake-selection

Internet Research Task Force. (Ed.). (2020). *Measurement and analysis for protocols research group (MAPRG)*. Retrieved from https://datatracker.ietf.org/rg/maprg/about/

Internet Society. (Ed.). (2018). *State of IPv6 deployment 2018*. Retrieved from https://www.internetsociety.org/resources/2018/state-of-ipv6-deployment-2018/

ISO/IEC JTC 1/SC 27. (2013a). Information technology – Security techniques – Code of practice for information security controls (second ed.). ISO 27002:2013. Retrieved from https://www.iso27001security.com/html/27002.html

ISO/IEC JTC 1/SC 27. (2013b). Information technology – Security techniques – Information security management systems – Requirements (second ed.). ISO 27001:2013. Retrieved from https://www.iso27001security.com/html/27001.html

ISO/IEC JTC 1/SC 27. (2018). Information technology – Security techniques – Information security risk management (third ed.). ISO 27005:2018. Retrieved from https://www.iso27001security.com/html/27005.html

Iyengar, J., & Thomson, M. (2019). *QUIC: A UDP-based Multiplexed and secure transport*. RFC. RFC Editor. Retrieved from https://datatracker.ietf.org/doc/draft-ietf-quictransport/

Jan, R. (2018). *How much of the Internet is using QUIC*. Ed. by APNIC. Retrieved from https://blog.apnic.net/2018/05/15/how-much-of-the-internet-is-using-quic/

Joint Task Force Transformation Initiative Interagency Working Group. (2013, April). Security and privacy controls for federal information systems and organizations. Retrieved from https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final

Jones, M., Bradley, J., & Sakimura, N. (2015, May). *JSON web token (JWT)*. RFC 7519. RFC Editor.

Kamara, S. (2016). Encrypted Search: Lectures 2+3: Provable Security. CS 2950-v (F'16). Brown University. Retrieved from http://cs.brown.edu/~seny/2950-v/2-provablesecurity.pdf

Korolov, M. (2019, February). What is biometrics? 10 physical and behavioral identifiers that can be used for authentication. Retrieved from https://www.csoonline.com/article/3339565/what-is-biometrics-and-why-collecting-biometric-data-isrisky.html

Kucherawy, M., & Zwicky, E. (2015, March). Domain-based message authentication, reporting, and conformance (DMARC). RFC 7489. RFC Editor.

Kuhlewind, M., Buhler, T., Trammell, B., Neuhaus, S., Muntener, R., & Fairhurst, G. (2017). A path layer for the internet: Enabling network operations on encrypted protocols. Retrieved from https://nsg.ee.ethz.ch/fileadmin/user_ upload/CNSM_2017.pdf

Laurie, B., Langley, A., & Kasper, E. (2013, June). *Certificate transparency*. RFC 6962. RFC Editor.

Lear, E., Droms, R., & Romascanu, D. (2019). *Manufacturer usage description specification*. RFC 8520. RFC Editor.

Leetaru, K. (2019, June). We must recognize just how Brittle and unpredictable todays correlative deep learning AI is. Retrieved from https://www.forbes.com/sites/kalevleetaru/2019/06/24/we-must-recognize-just-how-brittleand-unpredictable-todays-

correlative-deep-learning-ai-is/%5C?fbclid= IwAR2PN5l6Vox Jbl97N8DFlU4c9cux_ioxjSmZAvpKatvlAU_iIrkLx-lxCU8#2c 8ae5bb1a4a

Let's Encrypt. (Ed.). (2020). *Let's encrypt statistics*. Retrieved from https://letsencrypt.org/stats/

Leyden, J. (2018). *No Questions Asked', Windows code cert slingers 'fuel trade' in digitallysigned malware*. Ed. by The Register. Retrieved from https://www.theregister.co.uk/ 2018/06/26/digitally_signed_malware/

Livingood, J., Antonakakis, M., Sleigh, B., & Winfield, A. (2019, September). *Centralized DNS over HTTPS (DoH) implementation issues and risks*. RFC DRAFT. RFC Editor. Retrieved from https://datatracker.ietf.org/doc/draft-livingood-doh-implementation-risks-issues/

Lockheed Martin. (Ed.). (2015). *Lockheed martin cyber kill chain*. Retrieved from https://www.lockheedmartin.com/ content/dam/lockheedmartin/rms/documents/cyber/Gaining_ the_Advantage_Cyber_Kill_Chain.pdf

Lockheed Martin. (Ed.). (2019). *Small business suppliers learn cyber defense*. Retrieved from https://www.lockheedmartin. com/en-us/suppliers/news/features/2019/cybercorner-defense.html

Mandiant. (2019, July). *M-trends 2019: FIREEYE mandiant services special report*. Retrieved from https://content.fireeye. com/m-trends

Mandyam, G., Lundblade, L., Ballesteros, M., & O'Donoghue, J. (2019). *The entity attestation token (EAT)*. RFC. RFC Editor. Retrieved from https://datatracker.ietf.org/doc/draft-ietf-rats-eat/

Marin-Lopez, R., Lopez-Millan, G., & Pereniguez-Garcia, F. (2019). Software-defined networking (SDN)-based IPsec flow protection. RFC. RFC Editor. Retrieved from https://

datatracker.ietf.org/doc/draft-ietf-i2nsf-sdn-ipsec-flow-protection/

Mazieres, D., & Shasha, D. (2002, May). Building secure file systems out of Byzantine storage. TR2002–826. Retrieved from https://cs.nyu.edu/cs/faculty/shasha/papers/mazpodc.pdf

McKinnon, J. D., & MacMillan, D. (2018). Google says it continues to allow apps to ScanData from gmail accounts. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/google-says-it-continues-to-allow-apps-to-scan-datafrom-gmail-accounts-1537459989. Accessed on September 20, 2018.

Microsoft. (2019). Retrieved from https://www.microsoft.com/en-us/msrc/bounty

MITRE. (Ed.). (2017). Mitre attack. Retrieved from https://attack.mitre.org/resources/enterprise-introduction/

Moriarty, K., & Morton, A. (2018, July). *Effects of pervasive encryption on operators*. RFC 8404. RFCEditor.

Moriarty, K., & Richardson, M. (2019). *ACME overview*. RFC. RFC editor. Retrieved from https://datatracker.ietf.org/doc/draft-moriarty-acme-overview

Moriarty, K. M. (2019a). Coordinating attack response at internet scale 2 (CARIS2) workshop report. RFC. RFC Independent Stream Editor. Retrieved from https://datatracker.ietf.org/doc/draft-moriarty-caris2/

Moriarty, K. M. (2019b). *Cyber threat intelligence course, MPAI 775*. Retrieved from https://scs.georgetown.edu/programs/423/master-of-professional-studies-inapplied-intelligence/course-schedule/online/fall-2019

Moriarty, K. (2020). *ACME end user client and code signing certificates*. RFC. RFCEditor. Retrieved from https://datatracker.ietf.org/doc/draft-moriarty-acmeclient/

National Institute of Standards and Technology. (Eds.). (2018). *NIST cyber security framework overview page*. Retrieved from https://www.nist.gov/cyberframework

National Institute of Standards and Technology. (Eds.). (2020). NIST cryptography. Retrieved from https://www.nist.gov/topics/cryptography

NDSS Symposium. (Ed.). (2016, February). *TLS 1.3 ready or not (TRON) workshop programme*. Retrieved from https://www.ndss-symposium.org/ndss2016/tron-workshop-programme/

Neuman, C., Yu, T., Hartman, S., & Raeburn, K. (2005, July). *The kerberos network authentication service (V5)*. RFC 4120. RFC Editor.

Newman, L. H. (2018). A seemingly small change to chrome stirs big contreversy. *Wired*. Retrieved from https://www.wired.com/story/google-chrome-loginprivacy/. Accessed on September 24, 2018.

OneLogin. (2019). Retrieved from https://www.onelogin.com/

Open Identity. (2019). Retrieved from https://openid.net/

Padlipsky, M. A. (1982, September). *A perspective on teh ARPANET reference model*. RFC 871. RFC Editor.

Parker, M. (2018). Statement of issue with the cybersecurity jobs gap. CSO. Retrieved from https://www.csoonline.com/article/3258746/hiring-and-staffing/statement-of-issue-with-the-cybersecurity-jobs-gap.html. Accessed on 2018.

PCI. (Ed.). (2020). Payment card industry data security standard. Retrieved from https://www.pcisecuritystandards.org/

Pei, M., Atyeo, A., Cook, N., Yoo, M., & Tschofenig, H. (2019). *Trusted execution environment protocol (was open*

trust protocol). RFC. RFC Editor. Retrieved from https://datatracker.ietf.org/doc/draft-ietf-teepopentrustprotocol/

Plonk, D., & Berger, A. (2017, July). A measured approach to IPv6 address anonymization. Retrieved from https://arxiv.org/abs/1707.03900

Puppet. (2019). Retrieved from https://puppet.com/products/puppet-enterprise

Redfish Forum. (2019, August). *Redfish specification*. DMTF. Retrieved from https://www.dmtf.org/sites/default/files/standards/documents/DSP0266_1.8.0.pdf

Rescorla, E., Barnes, R., & Tschofenig, H. (2019). *Compact TLS 1.3*. RFC. RFC Editor. Retrieved from https://datatracker.ietf.org/doc/draft-rescorla-tls-ctls/

Rescorla, E. (2018, August). *The transport layer security (TLS) protocol version 1.3*. RFC 8446. Internet Requests for Comments.

Pei, M., Atyeo, A., Cook, N., Yoo, M., & Tschofenig, H. (2018). Protecting controlled unclassified information in nonfederal information systems and organizations Rev 1. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r1.pdf

RSA. (Ed.). (2019). RSA SecureID. Retrieved from https://www.rsa.com/en-us/products/rsasecurid-suite

RSA Conference. (2018). Network monitoring is going away... now what? TLS, QUIC, and beyond. Panel moderator. Retrieved from https://www.rsaconference.com/industry-topics/presentation/network-monitoringis-going-awaynow-what-tls-quic-and-beyond

Sangster, P., Khosravi, H., Mani, M., Narayan, K., & Tardo, J. (2008, June). *Network endpoint Assessment (NEA): Overview and requirements*. RFC 5209. RFC Editor.

Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., & Adams, C. (2013, June). *X.509 internet public key infrastructure online certificate status protocol -OCSP*. RFC 6960. RFC Editor.

Santesson, S., Myers, M., Ankney, R., Malpani, A., Galperin, S., & Adams, C. (2018, July). *Software inventory message and attributes (SWIMA) for PA-TNC*. RFC 8412. RFC Editor.

Security Services Technical Committee. (2005). Security assertion markup language (SAML). OASIS. Retrieved from https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

Sedgewick, A., Souppaya, M., & Scarfone, K. (2015, October). Guide to application whitelisting. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf

Selander, G., Mattsson, J., & Palombini, F. (2019). *Ephemeral diffie-Hellman over COSE (ED-HOC)*. RFC. RFC Editor. Retrieved from https://datatracker.ietf.org/doc/draftselander-lake-edhoc/

Selander, G., Mattsson, J., Palombini, F., & Seitz, L. (2019, July). *Object Security for constrained RESTful environments (OSCORE)*. RFC 8613. RFC Editor.

Sermersheim, J. (2006, June). *Lightweight directory access protocol (LDAP): The protocol*. RFC 4511. RFC Editor.

Sheffer, Y., Holz, R., & Saint-Andre, P. (2015, May). *Recommendations for secure Use of transport layer security*

(TLS) and datagram transport layer security (DTLS). RFC 7525. RFC Editor.

Shibboleth. (2020). Retrieved from https://www.shibboleth.net/

Smyslov, V., & Wouters, P. (2015, August). *The NULL authentication Method in the internet key exchange protocol version 2 (IKEv2)*. RFC 7619. RFC Editor.

Software Engineering Institute. (Ed.). (2020). Uber eXtensible Micro-Hypervisor Framework. Retrieved from https://uberxmhf.org/

Suppoya, M., Morello, J., & Sarfone, K. (2017, September). NIST special publication 800-190: Application container security guide. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-190.pdf

ten Oever, N., & Cath, C. (2017, October). *Research into human rights protocol considerations*. RFC 8280. RFC Editor.

The Decentralized Identity Foundation. (Ed.). (2020). The decentralized identity foundation. Retrieved from https://identity.foundation/

The OWASP Foundation. (Ed.). (2017). OWASP Top 10-2017, The ten most critical web application security risks. Retrieved from https://www.owasp.org/index.php/Category. OWASP_ Top_Ten_Project.

Tripwire. (Ed.). (2020). Retrieved from https://www.tripwire.com/

Unbound. (Ed.). (2019). *Unbound*. Retrieved from https://www.unboundtech.com (visited on 2019).

US Computer Emergency Response Team. (2018, March). Alert (TA18-074A): Russian government cyber activity targeting

energy and other critical infrastructure sectors. Retrieved from https://www.us-cert.gov/ncas/alerts/TA18-074A

Waltermire, D., & Fitzgerald-McKay, J. (2018). Transitioning to the security content automation protocol (SCAP) version 2. Ed. by National Institute of Standards and Technology. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.09102018.pdf

Waltermire, D., Quinn, S., Booth, H., Scarfone, K., & Prisaca, D. (2018, February). The technical specification for the security content automation protocol (SCAP) SCAP v1.3. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf

Westin, A. (1967). *Privacy and freedom*. New York, NY: Atheneum Press.

Wikipedia. (Ed.). (2020a). Wikipedia overview of microservices. Retrieved from https://en.wikipedia.org/wiki/Microservices

Wikipedia. (2020b). MINIX. Ed. by Wikipedia. Retrieved from https://en.wikipedia.org/wiki/MINIX

Wikipedia. (2020c). The delphi method. Ed. by Wikipedia. Retrieved from https://en.wikipedia.org/wiki/Delphi_method

Wooten, D., Proudler, G., & Aigner, R. (2016, December). Trusted platform architecture hard-ware requirements for a device identifier composition engine. Committee draft family 2.0, Level 0.0, revision 1.16. Trusted Computing Group.