Does Trust Still Matter in the Era of Zero Trust?

The most common theme of recurring security incidents in recent memory has been associated with the breaches of seemingly trustworthy service providers or technologies. It is causing major trust issues for organizations and consumers as to whether they are receiving adequate reassurance from the providers with whom they work. Understanding the shortfalls of existing security approaches, the probable enhancements using zero trust architecture and the use of relevant control frameworks can aid organizations in protecting against security incidents.

Revisiting the CIA Triad

Whenever information security has been discussed in the last four decades, the confidentiality, integrity and availability (CIA) triad, first laid out in 1976, is inevitably referenced.[1, 2] But how do these three principles apply to the systems, networks, operators or external factors of the IT professional's world? For example, the automated teller machine (ATM) was a great technological achievement in1967, and everyone still expects it to be secure even after 50 years.[3] Because financial institutions are highly regulated industries, there is no doubt that an ATM would have all possible controls in place to provide the assurance of the CIA principles in terms of:

- Confidentiality with multifactor authentication (MFA) since a customer needs both a physical card and personal identification number (PIN) to use the service
- Integrity that the bank will ensure that all transactions are conducted honestly and without any tampering of user data
- Availability because it is accessible even when the bank branch is closed

However, there are well-known dilemmas with each of these CIA principles:

- Confidentiality has been challenged by card skimmers who place magnetic card readers over the ATM's real card slot and use false PIN keypads to record card data and the user's PINs.[4]
- Integrity was lost during the attack of card processing networks in 2017, when hackers and money mules made coordinated cash withdrawals from overseas ATMs.[5]
- Outages of underlying networks, which link ATMs back to the bank, are frequent and lead to ATM service interruptions.[6]

Based on these examples, these principles are ineffective if they are designed or addressed without the comprehensive context of risk. The US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-39 defines information security risk as:

Ar Kar Oo, CRISC, CISM, CCSP, CISSP, ITIL Foundation, PRINCE2
Is a security consulting manager at EY Australia. Prior to EY, he was a cybersecurity senior manager at INSEAD (Singapore), a top global business school. He plays a critical role in the operational and strategic security programs, ensuring the delivery of education services across four locations in France, Singapore, UAE, and the United States, and online learning platforms. Prior to INSEAD, he was the chief information security officer (CISO) of Flexible Engine, the public cloud service of Orange Business Services, and the practice lead for cloud security professional services. He also worked on various consultation and implementation projects in public and private sectors while at Accenture.

Enjoying this article?

- Read *Privacy by Design and Default: A Primer. www.isaca.org/Privacy-by-Design*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

> *The risk to organizational operations (including mission, functions, image and reputation), organizational assets, individuals, other organizations and the nation due to the potential for unauthorized access, use, disclosure, disruption, modification or destruction of information and/or information systems.*[7]

Not only does that definition reflect the importance of having good risk management, but it also highlights the implications risk can bring to a nation.

That definition can be further expanded to include the effect on the world when the risk leads to the exploitation and takeover of critical infrastructure sector services causing regional or global disruptions.[8, 9]

Increased Sophistication in Cyberattacks

Recent headlines of some of the most impactful advanced persistent threats (APTs) demonstrate the dedication of threat actors to conduct sophisticated attacks and leverage zero-day vulnerabilities, making the actual realization of risk with global disruption no longer a hypothesis.

At the end of 2020, cybersecurity communities around the world were shocked to learn that SolarWinds Orion software had been breached and was serving a back door via the compromised update to many organizations. This incident showed that it is possible to direct a well-resourced and focused adversary's efforts to find a common software that is widely used at US government agencies, critical infrastructure entities and private organizations while maintaining a low profile for several months.[10] Given the number of customers and the industry sectors that SolarWinds has, this was a security disaster specifically attacking a supply chain.[11] Microsoft has finally named the actor as Nobelium and attributed to it the SolarWinds attacks, the SUNBURST back door, TEARDROP malware, and related components.[12] If the Nobelium incident is regarded as a national attack, then the exploitation of Accellion File Transfer Appliance would be considered a global attack.[13, 14] Organizations from Australia, New Zealand, Singapore, the United Kingdom and the United States, including the Reserve Bank of New Zealand, the US State of Washington, the Australian Securities and Investments Commission, the Singaporean telecom Singtel, the law firm Jones Day, the Kroger US grocery store chain, and even the cybersecurity firm Qualys were victimized.[15] One can only imagine that this kind of attack could happen to public cloud services and affect countless other organizations. How did these attacks happen? SolarWinds and Accellion were not the only targets of high-profile hacks, but both SolarWinds and Accellion's customers were in critical infrastructure sectors, making these hacks more severe than others. In the case of SolarWinds, the principles of the CIA triad were affected as follows:

- Confidentiality was breached on 4 September 2019 when unauthorized access was made to SolarWinds's system.
- Integrity was compromised 12 September 2019 when the arbitrary codes were injected into the Orion software update.
- Availability was not affected because customers were still accessing the software regardless of the authenticity.[16]

In contrast, the Accellion attack threatened the availability of business data because the threat actor was linked to the ransomware outfit. Inevitably, the breaches at SolarWinds and Accellion are comparable by security professionals because they were regarded as trusted partners by customers. Has the trust been misplaced?

In March 2021, Microsoft released several updates for critical vulnerabilities affecting Exchange Server versions 2013, 2016 and 2019, which were being exploited as part of an attack chain. As the latest development associated with the multiple zero-day vulnerabilities of Microsoft Exchange, on-premise deployments showed that the radius of the impact continued to grow every two to three hours on the organizations worldwide. In some cases, at least 10 APT actors from different countries were targeting the same organization. It is clear from the timeline that from the moment the vulnerabilities were exploited to the mass exploitation, there was not much time needed for them to escalate and weaponize.[17]

Another example occurred at Cisco Systems. A former employee of Cisco Systems was able to delete more than 400 virtual machines from

Amazon Web Services (AWS) five months after his resignation. Cisco guidelines for managing user access rights and offboarding procedures were flawed. The deletion caused an outage of 16,000 WebEx Team accounts for two weeks and cost the enterprise US$2.4 million.[18] Could it have been avoided? It was a breach of CIA principles.

Making Informed Decisions When Organizations Are Under Attack

In recent years, zero trust has been mentioned everywhere, including zero trust security, zero trust network and zero trust architecture. Created in 2010, the concept of zero trust is becoming increasingly popular and many vendors support its model.[19] At its core, the concept is based on an adage of "trust, but verify." However, more recently, refined architecture and deployment models have been created to address this concept. The reasons existing security models are not up to the task of evaluating trust and the means to improve them are well documented. Some of the pitfalls include:

- It is impossible to identify "trusted" interfaces.
- The mantra "trust, but verify" is not taken seriously.
- Malicious insiders are often in positions of trust.
- Trust does not apply to packets.

It may be an instinctive behavior for people to not verify data if they come from "presumably trusted" sources. However, there are three fundamental concepts to build the zero trust model:

1. Ensure that all resources are accessed securely regardless of location.
2. Adopt a least privilege strategy and strictly enforce access control.
3. Inspect and log all traffic.

Zero Trust Architecture

To broaden the adoption and understanding of the zero trust model, NIST published SP 800-207 with various approaches, deployment use cases and possible migration plans to achieve a zero trust architecture.[20] Deploying a zero trust architecture in an enterprise network is different and can be done by following specific business processes, giving flexibility and promoting user acceptance. Zero trust architecture includes three core components:

1. The policy engine is responsible for deciding to grant access to a resource for a given subject.
2. The policy administrator is responsible for establishing and shutting down the communication path between a subject and a resource.
3. The policy enforcement point is responsible for enabling, monitoring and eventually terminating connections between a subject and an enterprise resource.

> "IT MAY BE AN INSTINCTIVE BEHAVIOR FOR PEOPLE TO NOT VERIFY DATA IF THEY COME FROM 'PRESUMABLY TRUSTED' SOURCES."

Other components that act as data sources to provide input and policy rules used by the policy engine for making decisions include the following:

- Continuous diagnostics and mitigation (CDM) system
- Industry compliance system
- Threat intelligence feed
- Network and system activity logs
- Data access policies
- Enterprise public key infrastructure (PKI)
- Identification management system
- Security information and event management (SIEM) system

There are four zero trust architecture deployment models:

1. **Device agent/gateway-based deployment**—The policy enforcement point is divided into two components that reside on the resource or as a component directly in front of a resource. This model is most suitable for organizations with a robust device management program that can be used to implement agent/gateway in issued devices.

2. **Enclave-based deployment**—A variation of device agent/gateway-based deployment, the gateway components may not reside on assets or in front of individual resources but at the boundary of a resource enclave. This model is useful in legacy applications or on-premises data centers when individually deploying an agent is considered a challenge.
3. **Resource portal-based deployment**—The policy enforcement point is a single component that acts as a gateway for subject requests. The gateway portal can be for an individual resource or a secure enclave for a collection of resources used for a single business function. The limitation of this model is the visibility of the resource activities as it depends on whether the assets connect to the portal.
4. **Device application sandboxing**—This variation of the agent/gateway deployment model depends on only running trusted applications as a sandbox. It provides compartmentalization of assets in the form of virtualization and containerization to protect the host.

Common Criteria

In response to supply chain attacks, the updated NIST SP 800-53 can be used to help manage supply chain risk with policies and procedures, plans and controls, and processes.[21] IT professionals often spend a considerable amount of time ensuring that certain systems are accredited under Common Criteria (CC) and comply to Evaluation Assurance Level (EAL) three or higher.[22] While these accreditations are not the only approach to provide security assurance, both are efficient methods to

Figure 1—The Common Criteria 2021 Statistics

1564 Certified Products by Category *

Category	Products	Archived
Access control devices and systems	25	114
Biometric systems and devices	0	3
Boundary protection devices and systems	40	184
Data protection	64	139
Databases	12	75
Detection devices and systems	7	66
ICS, smart cards and smart card-related devices and systems	570	918
Key management systems	6	46
Mobility	25	42
Multifunction devices	228	248
Network and network-related devices and systems	219	405
Operating systems	47	155
Other devices and systems	234	529
Products for digital signatures	46	86
Trusted computing	41	16
Totals:	**1564**	**3026**
Grand Total:		**4590**

** A certified product may have multiple categories associated with it.*
Source: Common Criteria, "Certified Products List—Statistics," March 2021, *https://www.commoncriteriaportal.org/products/stats/*

evaluate and design critical components that are clear demonstrations of compliance to international standards complementing other certifications such as International Organization for Standardization (ISO) ISO 27001 or SOC 2. This EAL reinforces the trust between providers and customers located in different countries since CC can follow a country-specific scheme. The 2021 statistics on CC-certified products show that there are 1,564 active products in 14 categories. **Figure 1** illustrates the number of CC-certified active products in 2021 for each CC category.[23]

Cloud Security Alliance Cloud Controls Matrix
Many organizations now use at least one type of cloud service such as Software as a Service (SaaS), Infrastructure as a Service (IaaS) or Platform as a Service (PaaS), and that impedes the effectiveness of CC. The CC scheme was tailored to provide assurance for traditional software provisioning models, and, consequently, it is not well suited for service-oriented architecture (SOA) of cloud services because it is difficult to define the target of evaluation (TOE) or to delegate the operational environment (OE).[24]

Fortunately, this gap can be filled by leveraging the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) cybersecurity control framework that aligns to the CSA Best Practices and is considered the *de facto* standard for cloud security and privacy.[25] The 2021 revised CCM is robust enough to cover 17 important domains and is compatible with other frameworks such as ISO 27001:2013, ISO 27017:2015, ISO 27018:2019 and NIST SP 800-53.

Conclusion

It is important to build and maintain a trust relationship between providers and customers because one cannot exist without the other. Service providers and enterprises should adopt appropriate zero trust architecture deployment models and be transparent about their compliance to industry best practices. There will always be threats to diminish trust, but mutual understanding and assurance still can be accomplished using frameworks such as CSA CCM and by prioritizing continuous evaluation and improvements such as the CC EAL accreditation to facilitate verification. When in doubt, never trust, always verify.

"IT IS IMPORTANT TO BUILD AND MAINTAIN A TRUST RELATIONSHIP BETWEEN PROVIDERS AND CUSTOMERS BECAUSE ONE CANNOT EXIST WITHOUT THE OTHER."

Endnotes

1 Electricfork, "CIA Triad," 1 March 2010, *http://blog.electricfork.com/2010/03/cia-triad.html*
2 The MITRE Corporation, *Secure Computer System: Unified Exposition and Multics Interpretation,* USA, March 1976, *https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/bell76.pdf*
3 Weinberger, J.; "Protecting ATM Connections: Amid Security Threats, End Users Must Consider IoT and M2M," *Security Today*, 1 August 2017, *https://securitytoday.com/articles/2017/08/01/protecting-atm-connections.aspx*
4 Krebs, B.; "All About Skimmers," KrebsonSecurity, *https://krebsonsecurity.com/all-about-skimmers/*
5 Positive Technologies, "How Hackers Rob Banks," 21 May 2018, *https://www.ptsecurity.com/ww-en/analytics/banks-attacks-2018/?sphrase_id=85261*
6 Abrams, L.; "TD Bank Suffered Systemwide Banking Outage, Services Now Recovered," *Bleeping Computer*, 25 February 2021, *https://www.bleepingcomputer.com/news/technology/td-bank-suffered-systemwide-banking-outage-services-now-recovered/*
7 National Institute of Standards and Technology (NIST), NIST Special Publication (SP) 800-39 *Managing Information Security Risk: Operation, Mission, and Information System View*, USA, March 2011, *https://csrc.nist.gov/publications/detail/sp/800-39/final*
8 US Cybersecurity and Infrastructure Security Agency (CISA), "US Critical Infrastructure Sectors," *https://www.cisa.gov/critical-infrastructure-sectors*
9 UK National Cyber Security Centre, "CNI Hub," *https://www.ncsc.gov.uk/section/private-sector-cni/cni*

10 US Cybersecurity and Infrastructure Security Agency (CISA), Alert (AA20-352A): *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations*, USA, 17 December 2020, *https://us-cert.cisa.gov/ncas/alerts/aa20-352a*

11 Jankowicz, M.; C. Davis; "These Big Firms and US Agencies All Use Software From the Company Breached in a Massive Hack Being Blamed on Russia," *Business Insider*, 14 December 2020, *https://www.businessinsider.com/list-of-companies-agencies-at-risk-after-solarwinds-hack-2020-12*

12 Microsoft Security Response Center, "Nobelium Resource Center—Updated March 4, 2021," 21 December 2020, *https://msrc-blog.microsoft.com/2020/12/21/december-21st-2020-solorigate-resource-center/*

13 US Cybersecurity and Infrastructure Security Agency (CISA), Alert (AA21-055A): *Exploitation of Accellion File Transfer Appliance*, USA, 24 February 2021, *https://us-cert.cisa.gov/ncas/alerts/aa21-055a*

14 Accellion, *File Transfer Appliance (FTA) Security Assessment*, FireEye, USA, 1 March 2021, *https://www.accellion.com/sites/default/files/trust-center/accellion-fta-attack-mandiant-report-full.pdf*

15 Hay Newman, L.; "The Accellion Breach Keeps Getting Worse—and More Expensive, *Wired*, 8 March 2021, *https://www.wired.com/story/accellion-breach-victims-extortion/*

16 Sudhakar, R.; "New Findings From Our Investigation of SUNBURST," Orange Matter, 11 January 2021, *https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/*

17 Faou, M.; M. Tartare; T. Dupuy; "Exchange Servers Under Siege From at Least 10 APT Groups," WeLiveSecurity, 10 March 2021, *https://www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/*

18 itNews, "Ex-Cisco Engineer Deleted 456 VMs for Webex Teams After Exit," 27 August 2020, *https://www.itnews.com.au/news/ex-cisco-engineer-deleted-456-vms-for-webex-teams-after-exit-552494*

19 Kindervag, J.; *No More Chewy Centers: Introducing the Zero Trust Model of Information Security*, Forrester, 17 September 2010, *https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf*

20 Rose, S.; O. Borchert; S. Mitchell; S. Connelly; Special Publication (SP) 800-207, *Zero Trust Architecture*, National Institute of Standards and Technology (NIST), USA, August 2020, *https://csrc.nist.gov/publications/detail/sp/800-207/final*

21 National Institute of Standards and Technology (NIST), NIST Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*, USA, September 2020, *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*

22 Common Criteria, *https://www.commoncriteriaportal.org/cc/*

23 Common Criteria, "Certified Products List – Statistics," *https://www.commoncriteriaportal.org/products/stats/*

24 Kaluvuri, S. P.; M. Bezzi; Y. Roudier; "Bringing Common Criteria Certification to Web Services," 2013 IEEE International Workshop on Security and Privacy Engineering, Assurance and Certification, *https://www.eurecom.fr/en/publication/4092*

25 Cloud Security Alliance, Cloud Controls Matrix v4, *https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/*