Is STIX (Structured Threat Information eXpression) an appropriate technology for the world finance communtiy?

William Abbott Foster, PhD, Georgia Tech (william.foster@inta.gatech.edu)
Hannah Thoreson
Xiaowen Xu

Introduction

Cybersecurity is a field whose methods are becoming extremely difficult to implement as the number and types of digital devices connected to the internet continue to proliferate. While one may traditionally consider cybersecurity as a field centered around PC's and servers, the potential targets for attackers now also include smartphones, tablets, and numerous other devices open to exploitation. This has created a problem where standards and implementation schemes across the expanding range of technologies are not always compatible, and as a result solutions to cybersecurity problems typically require a lot of individual attention from IT workers. Efficiency is out of the question, and security is weakened as a result. STIX is designed to take the opposite approach, and "maximize structure and consistency to support machine-processable automation" (10).

STIX is one approach that could possibly act to mitigate some of these problems. STIX is managed by the MITRE Corporation, a nonprofit that manages federally-funded research centers, and sponsored by the Department of Homeland Security. Its explicit aim is to assist in defending critical U.S. infrastructure from attack. The financial system is a prime target for enemies of the U.S. government. For example, it is believed that Iran is most likely behind a recent wave of attacks on the financial industry (Perlroth & Hardy, 2012). A more successful disruption of American commerce by a foreign power would be devastating.

Functionality of STIX

STIX, or the Structured Threat Information eXpression, is a language "meant to convey the full range of cyber threat information and strives to be fully expressive, flexible, extensible, automatable, and as human-readable as possible" (The MITRE Corporation, 1). At least at this point, STIX currently exists as a programming language within a programming language. It is a specialized XML schema that has been developed with the primary purpose of "tagging" various aspects of a successful or attempted exploit (MITRE, 5). The data can then be collected, shared, and used by systems or organizations using a common standard for formatting the information. STIX is practical, because it leverages existing standardized language where appropriate; for example, in its representation of observables, it leverages the CybOX standardization effort (MITRE, 12). It also is designed such that everything in STIX is optional for the end user.

STIX “is intended to provide full expressivity for all relevant information within the cyber threat domain”. As such, it is designed to be helpful when performing a wide range of tasks, as opposed to emphasizing only a narrow band of the cybersecurity realm. For example, STIX is useful for analyzing cyber threats, because it has a structured, standardized way to find and collect the data on an attack. It is also helpful in specifying indicator patterns for cyber threats, taking preventative courses of action for relevant threats, monitoring cyber operations, and responding to incidents (MITRE, 8). STIX is also extensible in case a user finds its toolbox to be incomplete (MITRE, 10).

The way STIX achieves these goals is by identifying the data objects that could be collected about an attack, and then fleshing out those constructs in detail within the XML schema housing the language (MITRE, 11). The eight “core constructs” that MITRE identified when developing STIX are the Observable, Indicator, Incident, TTP (Tactics, Techniques, & Procedures), ExploitTarget, CourseOfAction, Campaign, and ThreatActor (11). STIX leverages existing standards when defining observables and indicators. However, it develops its own language for all or part of the other core constructs as no adequate standards currently exist.

STIX and Trusted Relatonships

Trust is extremely important in cybersecurity in order to enable sharing of information about threats and security breaches between institutions. Unfortunately, there is a major lack of trust between corporations, between the private sector and government, and between U.S. organizations and those belonging to countries outside the West. Companies often like to keep security information private, as making their vulnerabilities known may cause them to lose customers (Bipartisan Policy Group, 9). There are also legal concerns surrounding information sharing in the U.S (Bipartisan Policy Group, 9). Data must be handled in a way that respects consumers’ privacy and civil liberties (Bipartisan Policy Group, 5). Companies are also often loath to collaborate with the government, which makes it difficult for security agencies to develop practical strategies for protecting U.S. infrastructure (Harwood, 2011). All of this is to say nothing of the borderline-hostile relationship between U.S. cybersecurity agencies and their foreign counterparts, which creates an environment that is not at all conducive to sharing information about threats and attacks.

These drawbacks are some of the reasons that in the past, MITRE has developed other cybersecurity products which never saw much practical use. These products may be very technologically advanced but ignored by private industry. Part of the reason for this may also be that private industry is often reluctant to inorganically adopt a new standard. One of the most popular language in private-sector software development is still C++, which was developed in 1983 by a landline telephone service provider (AT&T, 2013). Since so many programmers learn and are trained in the most popular languages and procedures, and so many companies are familiar with them, it becomes difficult for new languages to see widespread adoption.

World Financial Community

Cybersecurity is of particular concern to the world financial community. One might imagine that the greatest cyber threat faced by banking institutions would be criminals looking to steal money or conduct some kind of fraud, but the financial system is also considered a critical piece of infrastructure that hackers from terrorist groups, hostile governments, and other less materially-focused groups may target (George 1). In fact, dozens of American banking sites were recently attacked by hackers tied to the government of Iran (Perlroth 2013). An attack of this nature is performed mainly with the intent of causing a disruption in commerce or the economy rather than to steal funds (Perlroth 2013).

The financial industry has been at the forefront of cybersecurity efforts, and has at least one organization dedicated to sharing threat information, the Financial Services Information Sharing and Analysis Center [FS-ISAC] (George 9). There are also numerous public-private partnerships in information sharing between the financial industry and the federal government (George 9). These organizations could help to make STIX the standard cybersecurity technology used by their industry in the United States (George 9).

China and a worldwide implementation of STIX in the Financial Community

As China develops fast in information technology and the Internet industry and is inflicted with rampant hacking activities, it is high time U.S. and China built cooperation in cyber security protection. However, the lack of trust among the two nations raises the biggest difficulty for the bilateral cooperation on information security. For years, U.S. government has condemned China of intrusions into economic and national security database and networks with all kinds of hacking activities.

In November 2006, the Financial Services Information Sharing and Analysis Center and five banks in U.S. noticed fierce attacks in their networks. Soon China was found to base these attacks (Sausner, 2007). In 2011, U.S. corporations and cyber security specialists reported an attack of computer network originating from IP addresses in China (James, 2011). China-based hackers were also discovered penetrating the computer networks of the White House, president campaign groups, and the Pentagon's defenses (Sevastopulo, 2008). According to private cyber security specialists, some of these computer attacks used Chinese government websites to download malicious code (Fidler, 2007). Despite all these speculations, because the malwares and botnets detected in these cases do not need government-level support, no one could say definitely that China's government has a hand in them. It was also possible that Chinese servers are only the final hopping point for a disguised American hacker (Sausner, 2007). Two leading Chinese telecom manufacturers, ZTE and Huawei, also failed to escape a charge from the U.S. Congress of embedding spyware in supplies in 2009. They have been excluded from U.S. government contracts (*Financial Express*, 2012). In early 2010, the U.S. search giant Google complained “highly sophisticated and targeted attacks” originating from China, which caused it to move its Chinese service from mainland China to Hong Kong (James, 2011).

Similar incidents have also been reported by Canada and some European countries, which impaired China’s reputation in international cooperation. In April, 2009, GhostNet, which had intruded more than one thousand computers in 103 countries in less than two years with a target on the Dalai Lama and Tibetan government-in-exile, was accused by experts in Britain of being conducted by China-based computers (*Economist*, 2009)

Many experts and officials in U.S. express implicit or explicit suspicion towards Chinese government. Richard Clarke, the former Cyber-security Czar in George W. Bush’s government and expert on cyber war, denounced China's government and its industries for the espionage activity in 2011. He even suspected China of funding other countries on stealing of trade secrets and research (Ho, 2011). Others lathe to firmly say so, but still caution for the significant threat. "They (Chinese) represent a very high threat because they're a nation state, because they have means, motive and opportunity, because they're well-resourced and patient," says O. Sami Saydjari, president and founder of Cyber Defense Agency, a cyber security consultancy (Sausner, 2007).

In 2011, the Office of the National Counterintelligence Executive (ONCIX) identified in a report that Chinese and Russian businesses and governments as potential information and secrets collector as the relationship between U.S. and foreign companies is strengthened (Smith, 2011). Posited by some, such as House Intelligence Chairman Mike Rogers, R-Mich., intellectual property theft from commercial competitors may be the possible motivation for China’s hackers, if it is the case (Smith, 2011). Whether it is a part of the plot, the reluctance of Chinese government to probe further as a host country and incapability to consolidate cyber security further instigates U.S. (*Economist*, 2009).

Another fatal problem which hampers mutual trust is the lack of protection for privacy and data, and weak contract system in China. This drawback becomes even more critical in financial security, which deters the motivation of international corporations or financial entities. There are institutional and legal loopholes in public information safety, and an effective management mechanism still waits to be set up (Zhao & Wang, 2010).

Faced with a series of accusation, Chinese government keeps denying linkage to these cyber-crimes. China responded that the label of "the world's most active and persistent perpetrators of economic espionage" by ONCIX is “baseless”. Chinese Foreign Ministry spokesman Hong Lei said that “identifying the attackers without carrying out a comprehensive investigation and making inferences about the attackers are both unprofessional and irresponsible" (James, 2011). Yang Jiechi, China's foreign minister, also denied government support for hackers targeting UK companies, which is prohibited by Chinese law (Fidler, 2007). These conflicts in cyberspace also undermines China’s trust in U.S.. Recent advancements in cyber technology of U.S. elicit more cautions from China, referred to as “Cold War thinking” (Sevastopulo, 2008). According to the foreign relations scholar in Fudan University, Cai Cuihong, China believes U.S. is attempting to control the hegemony in the “uncharted territory” of the cyber space, in order to maintain its leading status in technology, military and economy, solidify territory, and to disseminate its culture and values (Cai, 2012; also see Shen, 2010; Lu, 2012). It endeavors to construct and strengthen international codes and rules for cyber space and involve allies into this favorable system. Compared to this precursor in cyberspace, China is disadvantaged in competing for technology innovation and resources (Liu & Huang, 2012). Furthermore, the ongoing conflicts in intellectual property, Internet censorship, ideology and values exacerbate the "trust deficit" and difficulty for collaboration (Cai, 2012). Yi Wenli, the assistant researcher in the National Research Center for Information Technology Security in China, stated that the distrust between China and U.S. politicizes the legal issues of cyber-crimes and hinders mutual rapport in relevant area (Yi, 2012).

The U.S. department of Defense and the Chinese People's Liberation Army (PLA) both perceive cyberspace as a rising strategic field for global competition, and hold strong stance on cyber security (University of California, Institute on Global Conflict and Cooperation (IGCC), 2012). This may be the hardest barrier prevent deep cooperation. Security specialists say Chinese intelligence-gathering officially is carried out either by the third department of the general staff of the People's Liberation Army managing communication infrastructure or by the Ministry of State Security (Fidler, 2007). The military sector in China worries that the expansion of U.S. power in cyber space would fuel virtual military contest in the future. Moreover, the revolution in the Middle East is perceived as stimulated by the Internet technology and U.S. intervention in domestic politics in other countries. Recent construction of the Cyber Command, release of the National Security Strategy, and more active cyber deterrence strategy in U.S. pose greater threat towards China. PLA leaders and strategists are reported to pay close attention to the military applications of information technology, and U.S. doctrine and practice in military area (Lu, 2012; Liu & Huang, 2012).

Harassed by ballooning Website defacements, access denials, and network intrusions, international cooperation in cyberspace is actually within the interests of both U.S. and Chinese governments. However, how to break the ice of cyber cooperation between China and U.S. is not easy. Although Chinese Communist Party in China centralizes the political power, Chinese political regime is fractured regionally and functionally: various public and private sectors have conflicting interests, implementing regulatory institutions and policies inconsistently (University of California, IGCC, 2012). This fragmentation in administration is also the case in cyber security field. The lack of a central level government body or organization specifically on cyber security issues increases the difficulty of high-leveled and integrated activities.

One possible approach is through the negotiation and coordination between the academic and financial bodies to gradually attenuate rivalry from military sectors on both sides, such as "track II" diplomacy. Through such cooperation, we can discuss the basic principles, cooperation framework and mechanism. This approach may work well especially in China. In Chinese culture, trust (*xin ren*, *hu xin*) is easily built on friendship, *guan xi* (social network) and *ren qing* (human feelings). Thus, unofficial communication and public diplomacy are promising mechanisms to smooth the bilateral relationship. In academic and research field, at least National Computer Network Emergency Response Technical Team (CNCERT) under MIIT

(Ministry of Industry and Information Industry) is trusted by USCERT and CERTS program around the world, and is a member of Forum of Incident Response and Security Teams (FIRST). It may be possible to lead the dialogue process within this field. In fact, the experts in CNCERT said that China has been confronted serious cyber-attacks from domestic and external threat, and appealed to deepened international cooperation in this area (*Xinhua News*, 2012).

Russia

http://www.fas.org/pubs/pir/_docs/2012Spring_Multilateral_Cybersecurity_Solutions.pdf
Under what situation would the Russian government use STIX to shutdown hacks from the cybermafia in Russia and Eastern Europe on the world financial community.

ITU

The International Telecommunications Union (ITU) is not an

See article by Rutkowsi, Foster, and Goodman

http://www.fas.org/pubs/pir/_docs/2012Spring_Multilateral_Cybersecurity_Solutions.pdf

Conclusion

STIX is a technology that would be suitable for exchanging threat information in the financial industry. However, trust issues within various communities that comprise the global financial community may impede the adoption of a new standard without organic support for such an initiative.

Works Cited

Perlroth, N. and Hardy, Q. Bank Hacking Was the Work of Iranians, Officials Say. Retrieved from www.nytimes.com/2013/01/09/technology/online-banking-attacks-were-work-of-iran-us-officials-say

Cai, C. (2012). Sino-U.S. relations in cyberspace: Competition, conflict, and cooperation, *Meiguo yanjiu (American Studies)*, 3, 107-121.

China is becoming the biggest victim of cyber-attack, prompting deepening international cooperation (2012, Jul. 4). *Xinhua News*. Retrieved from http://news.xinhuanet.com/politics/2012-07/04/c_112357660.htm

Fidler, S. (2007, Dec. 6). Steep rise in hacking attacks from China: [ASIA EDITION]. *Financial Times*, 8. Retrieved from http://ezproxy.msu.edu.proxy1.cl.msu.edu/login?url=http://search.proquest.com.proxy1.cl.msu.edu/docview/250068726?accountid=12598

Ho, V. (2011, Apr. 23).

Industrial espionage has a new bogeyman. *The Business Times*. Retrieved from http://ezproxy.msu.edu.proxy1.cl.msu.edu/login?url=http://search.proquest.com.proxy1.cl.msu.edu/docview/863030183?accountid=12598
International:

A Chinese ghost in the machine?; Cyberwarfare (2009, Ap. 4). *The Economist, 391,* 62. Retrieved from http://ezproxy.msu.edu.proxy1.cl.msu.edu/login?url=http://search.proquest.com.proxy1.cl.msu.edu/docview/223987306?accountid=12598

Liu, B. & Huang, F. (2012). The gaming among political powers in international cyberspace, *Shehui zhuyi yanjiu (Socialism Studies), 3,* 120-126.

Lu, J. (2012). A review on Obama government's cyberspace security policy, *Guoji guancha* (*Internal Inspection), 2,* 23-29.

James, S. B. (2011, Nov 08). China reportedly denies charges of cyberattacks, economic espionage. *SNL Kagan Media & Communications Report.* Retrieved from http://ezproxy.msu.edu.proxy1.cl.msu.edu/login?url=http://search.proquest.com.proxy1.cl.msu.edu/docview/903324549?accountid=12598

Sausner, R. (2007, May). The New Red Menace, *Bank Technology News, 20(5),* 27. Retrieved from http://ezproxy.msu.edu.proxy1.cl.msu.edu/login?url=http://search.proquest.com.proxy1.cl.msu.edu/docview/208155054?accountid=12598

Sevastopulo, D. (2008, Nov 8). Hackers breach White House system. *Financial Times,* 6. Retrieved from http://ezproxy.msu.edu.proxy1.cl.msu.edu/login?url=http://search.proquest.com.proxy1.cl.msu.edu/docview/250161912?accountid=12598

Shen, Y. (2010). The intelligence, competition and cooperation in the digital space: The cybersecurity relations under the strategic framework of Sino-US relationship. *Waijiao pinglun* (*Diplomacy Critics), 2,* 38-47.

Smith, J. (2011, Nov. 3). Report: China, Russia Top Culprits in Cyber Espionage, National Journal. Retrieved from http://ezproxy.msu.edu.proxy1.cl.msu.edu/login?url=http://search.proquest.com.proxy1.cl.msu.edu/docview/902188307?accountid=12598

Spyware charge: China's Huawei slams US report (2012, Oct. 30). *Financial Express*.Retrieved from http://ezproxy.msu.edu.proxy1.cl.msu.edu/login?url=http://search.proquest.com.proxy1.cl.msu.edu/docview/1115585540?accountid=12598

University of California, Institute on Global Conflict and Cooperation (IGCC). (2012). *China and cybersecurity: Political, economic, and strategic dimensions* (Workshop Report on China and Cybersecurity).

Yi, W. (2012). The discrepancy and approach to cooperation between U.S. and China in cyberspace. *Dangdai guoji guanxi* (*Contemporary International Relations), 7,* 28-33.

Zhao, J., & Wang, S. (2010). On the Drawbacks and Improvement of Legal System of Supervision on Securities Fraud in Cyberspace in China, *Canadian Social Science,* 6(1), 40-44.

The MITRE Corporation. Standardizing Cyber Threat Intelligence Information with the Structured Threat Information eXpression (STIX™) White Paper. Retrieved from http://stix.mitre.org/about/documents.html

Bipartisan Policy Group. Cyber Security Task Force: Public-Private Information Sharing. July 2012.

Harwood, Matthew. Lack of Trust Thwarts Cybersecurity Information Sharing. February 23, 2011.

George, Kyle. Financial System Security. December 6, 2012.