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

An opportunity for US – Chinese collaboration?

by

William Abbott Foster, PhD, Hannah Thoreson, Xiaowen Xu

January 23, 2013

Biographies of Authors

William Abbott Foster, PhD is a Senior Research Associate with the Center for International Strategy and Policy (CISTP) at the Sam Nunn School of International Affairs at Georgia Tech in Atlanta, Georgia. He has twenty-five years of experience in government, industry, and academia building global collective intelligence systems to support engineering policymaking including around cyber-security. His books and articles are available on-line at http://www.fosterandbrahm.com. His email is william.foster@inta.gatech.edu Mailing address: William Abbott Foster, Sam Nunn School of International Affairs, Georgia Tech, 781 Marietta Street #315, Atlanta, GA 30318

Hannah Thoreson runs a company specializing in social media research. She has a bachelors degree in physics from Arizona State University where she was president of the College Republicans ASU chapter.

Xiaowen Xu is currently a graduate student in Communication Studies in Michigan State University. Her interest is in communication issues on the Internet and social media, and intercultural communication. Before coming to Michigan, she received the bachelor degree in Journalism in Tsinghua University in China, and master degree in East Asian Studies in Columbia University in New York City.

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

An opportunity for US – Chinese collaboration?

Abstract

In this article we argue that the Obama Administration should take the lead and have the US Department of Treasury reach out to the Chinese Banking and Regulatory Commission and the Peoples Bank of China to work together to make the world's financial system more resilient. The US government has funded the development by MITRE of a system for automated threat exchange to support critical US infrastructure. This XML based system, which has been presented to the Internet Engineering Task Force (IETF) at their Fall meeting in 2012, should be implemented quickly at a global level by building on and contributing to "trust" relationships in the world financial community, particularly the relationships between US and Chinese financial leaders.

Keywords

STIX, Cyber-Security, Financialm, US, China

Introduction

Cybersecurity is a field whose methods are becoming extremely difficult to implement in the face of advanced persistent threats. There has been a rapid evolution in the complexity of cyber-attacks and the ability of attackers to hit many networks simultaneously. Attacks are beginning to come in waves with a rapid succession of probing and attacking untill a network's security is breached. To further complicate matters, the rapid adoption of smartphones and tablets greatly increases the difficulties of defending a network.

The US government has funded the development by MITRE of the STIX automated threat sharing platform in an effort to address the new realities of cyber-attacks. STIX, which stands for Structured threat information eXpression, has been submitted to the Internet Engineering Task Force (IETF) in hopes to support widespread adoption in America's critical infrasture.

If you are interested in STIX it is highly recommended that you read MITRE's "Making Security Measurable" white paper available at http://makingsecuritymeasurable.mitre.org/docs/STIX-Whitepaper.pdf Mitre has developed a website for conveying developments about STIX. It is at http://stix.mitre.org/

MITRE has a long history of developing sophisticated security technology which though technically sophisticated is often never fully adopted by industry. We believe that our society faces a major cyber-security challenge, a challenge that US policymakers cannot address by focusing on US cyber-infrastructure. For example, the world's financial community is under widespread cyber-attacks that come from all over the world and require a global response.

Though many policymakers in Washington, DC believe that China cannot be trusted in cyber-relations, we propose that the Obama Administration reach out to its counterparts in the Chinese financial community (Peoples Bank of China and Chinese Banking and Regulatory Commission), the research community (Chinese Academy of Science), and the Chinese Cyber Emergency Response Team (CNCERT) and work together to implement STIX strategically in various parts of the world financial community.

We need to recognize that STIX must be implemented in the context of relationships of trust. In providing other organizations with insights into your vulnerabilities, you run the risk that that organization may use that information to attack you. Thus using STIX in connecting US and Chinese financial systems, has the potential of leading to an even greater breakdown of trust and the US – Chinese relationship, or it may result in "trust building" and the decision by the Chinese Communist Party to shutdown attacks on the US by the PLA and the hacker teams it works with.

We have evidence that the “financial” and “technical” officials in the Chinese Communist Party--some of whom have gotten their PhDs in the West and some of whom control Chinese $3 trillion in foreign reserves—have the ability to use a worldwide STIX implementation to shut down PLA and hacker attacks on the US.

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 (MITRE,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 Relationships

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, 2012, 9). There are also legal concerns surrounding information sharing in the U.S (Bipartisan Policy Group, 2012, 9). Data must be handled in a way that respects consumers' privacy and civil liberties (Bipartisan Policy Group, 2012, 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++ and Java. Since so many programmers learn and are trained in the most popular languages and procedures, there has been a surprising resistance to moving to an XML orientated strategy for ensuring that data is hardware and software independent.

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, 2012, 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 cyber-security efforts, and has at least one organization dedicated to sharing threat information, the Financial Services Information Sharing and Analysis Center [FS-ISAC] (George, 2012, 9). There are also numerous public-private partnerships in information sharing between the financial industry and the federal government (George, 2012, 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

It is high time U.S. and China collaborate 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).

In fact Barry Greene, former Chief Security Architect at CISCO, points out that there are things hackers in China can do and things they are not allowed to do. Greene claims that the Peoples Bank of China will not allow Chinese hackers to steal “credit card information” and “financial information “ from outside of China. The Peoples Bank of China is concerned that if such practices became rampant they would lose control of their “Great Financial Firewall of China (Interview at ISC, Greene, 2011)

Two leading Chinese telecom manufacturers, ZTE and Huawei, were accused by the U.S. Congress of embedding spyware in supplies and have been excluded from U.S. government contracts (*Financial Express*, 2012). Foster claims the US House Intelligence Committee was not able to find any evidence that Huawei or ZTE had placed backdoors in any of its customers network equipment or violated their customers trust. Foster believes that the two companies were scapegoated by US politicians. (Foster, 2012)

Chinese and US citizens grow up with very different expectations of who they can trust and how to develop “trusted relationships” Americans generally assume that signed contracts which are enforced by independent courts are the basis for trust. It is immensely frustrating, for Americans to find that they cannot rely on the rule of law to enforce a contract in China nor can the “courts” be trusted.

There have been numerous responses by Chinese officials to claims in Washington, DC that China cannot be trusted in cyber-security. Would there be a willingness in the State Council and in the Chinese Communist Party to collaborate with the United States to implement a security technology that was developed by the US government?

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).

The Chinese government is 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 mistrust between China and U.S. is not easy.

Though Chinese Communist Party in China on one hand centralizes political power, the 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 “track II diplomacy” with negotiation and coordination between the academic and financial bodies to gradually attenuate rivalry from military sectors on both sides.

This “relationship” based approach may work well especially with the Chinese. 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 coordination are the way to build a bilateral relationship.

The officials in the Chinese government with the responsibility of managing $3 trillion in foreign reserves and making sure that the Chinese banking system stays solvent have real incentives to work with the Obama Administration to protect the world’s financial system. The more they collaborate with their counterparts in the US the stronger the trust relationships between China and the US.

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).

ITU

Rutkowski, Foster,and Goodman (2012) argue that it is not wise to try and use the International Telecommunications Union (ITU) to centralize threat sharing and the development of global cyber-security standards. The United States and many other countries were concerned with proposals pushed by China and Russia at ITU’s World Conference on International Telecommunications 2012 (WCIT-12) in Dubai. It is appropriate for the ITU to work with other standards bodies such as the IETF, but there is a long history of the ITU, in the attempt to solve security problems, actually creating a breakdown in trust.

Conclusion

STIX is a technology that might be suitable for exchanging threat information in the global financial industry. However, there are many challenges. As former Citicorp CTO Amal Choudrey (Interview, 2011) points out, there is no global financial cloud and each financial institution defines what it wants to secure differently from what other types of financial institutions both in their country, but more importantly in other countries, think is important.

It is possible that STIX may not gain traction in the US, yet we argue that the Obama Administration as part of its cyber-security initiative reach out at a high level to the Chinese leadership to explore collaborating on implementing automated threat sharing in the world's financial community. Instead of leading to a further breakdown in trust, we believe that such collaboration will increase the level of trust between the US and Chinese government and is imperative for helping build trust in the world's financial system.

Works Cited

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

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

Foster, W (2012) William Abbot Foster, "Commentary: The US House Intelligence Committee Scapegoats Huawei", China Currents, December 20, 2012; Vol. 11, No. 2 Retrieved from http://www.chinacenter.net/commentary-the-u-s-house-intelligence-committee-scapegoats-huawei/

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

George, Kyle (2012) Financial System Security. A paper for a Georgia Tech course on cyber-security policy.

Harwood, M. (2011). Lack of Trust Thwarts Cybersecurity Information Sharing. February 23, 2011.

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

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

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.

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

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

Rutkowsi, Foster, and Goodman(2012), Multilateral Cybersecurity Solutions, PIR Spring, Retrieved from http://www.fas.org/pubs/pir/_docs/2012Spring_Multilateral_Cybersecurity_Solutions.pdf

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.