Protecting Critical Infrastructures: Financial Services Sector

Introduction

The American homeland is under attack. State and non-state actors are targeting vulnerabilities continually. This paper presents bleeding edge cyber and information warfare techniques to protect the financial services sector--one of America's critical infrastructures (Critical Infrastructure Sectors 2013) as defined by the Department of Homeland Security.

National security agencies, in collaboration with financial services sector stakeholders, should creatively and aggressively prototype novel defensive techniques. Power outages, physical and cyber attacks are palpable risks. "Essential to understanding the sector's cybersecurity and physical risks is the identification of critical processes and their dependence on information technology and supporting operations for the delivery of financial products and services" (Financial Services Sector-Specific Plan 2015). Process mining is a tool which can help steel America's critical infrastructures against these ongoing homeland threats.

Background

Process mining is a powerful artificial intelligence technique with expansive use cases throughout the corporate and government world. As the name implies, algorithms "mine" data and surface latent processes with no *a priori* knowledge. Compared to traditional process mapping methodologies, process mining learns processes more accurately and in a fraction of the time. It is fast, repeatable, and scalable.

Many types data may be mined potentially, providing insight into both the financial sector human operations as well as machine decision making processes. Insights into human operations are useful in social engineering attacks. Machine process insights are useful for identifying process weak points and systems near capacity, which could be subjected to Distributed Denial-of-Service (DDoS) attacks or attacks that closely simulate normal operations so as to avoid detection (Bicknell and Krebs 2019)

Importantly, event logs are process agnostic; nearly any data source which chronicles events is usable. Thus, there are vast amounts of data suitable for process mining. These data may be obtained from cybersecurity and related information system logs, daily regulatory filing data, Internet of Things networks, and social media activity. (Bicknell and Krebs 2019).

After extracting event details from these data using well known techniques, the resulting timestamped data are mined for latent processes to provide financial institutions and government analysts with actionable insights about process-related vulnerabilities in order to prioritize mitigation activities (Bicknell and Krebs 2019).

The remainder of this paper presents three techniques which the authors believe provide effective and scalable cyber and information defense in support of the financial services sector stakeholders.

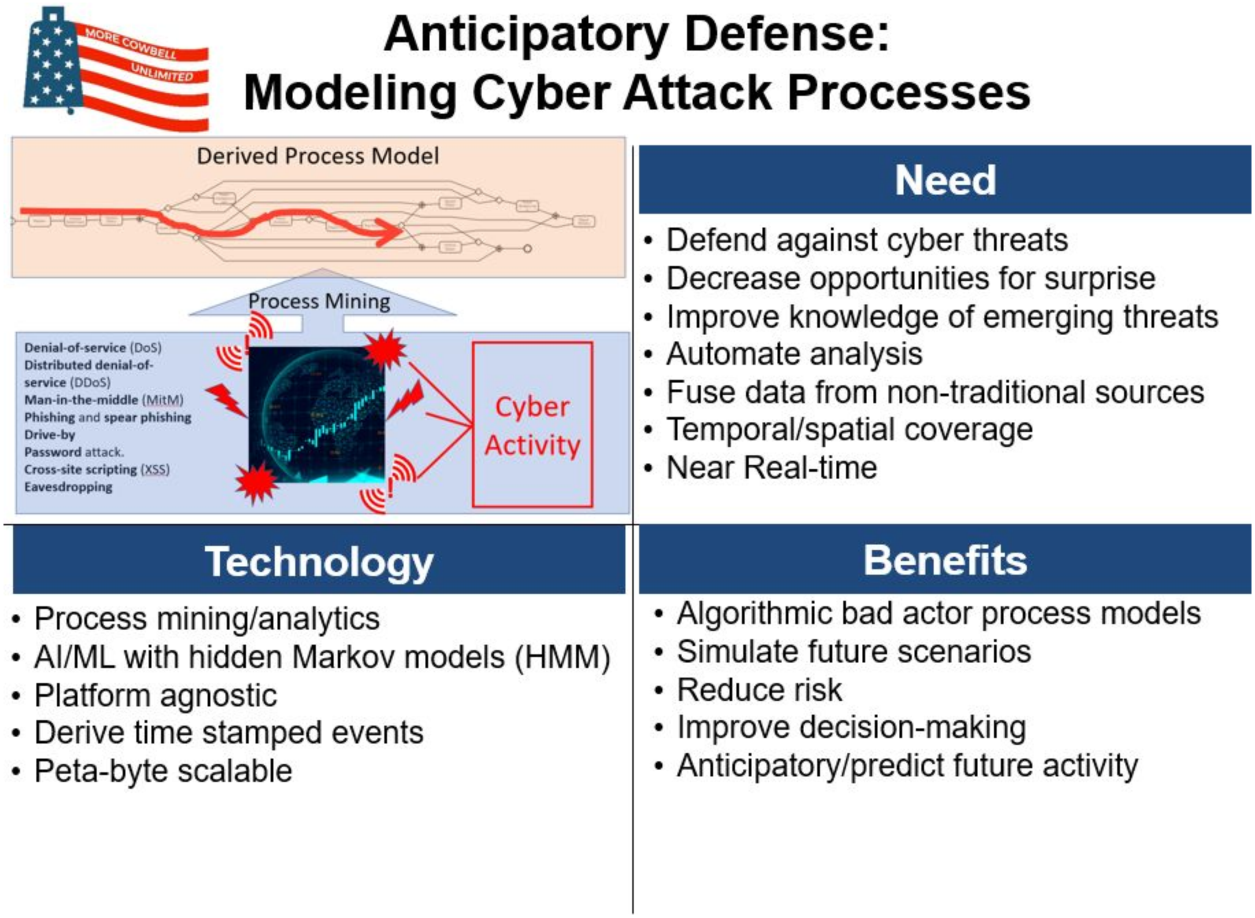
© 2019 Copyright More Cowbell Unlimited, Inc.

How to cite this article: Bicknell JW and Krebs WG (2019), "Protecting Critical Infrastructures: Financial Services Sector", More Cowbell Unlimited White Paper, retrieved from https://morecowbellunlimited.com/wp-content/uploads/Protecting-Critical-Infrastructures-Financial-Services.pdf

Anticipatory Defense: Modeling Cyber Attack Processes

America’s critical infrastructure--including the financial services sector--is under constant cyber attack. The United States government and financial corporations monitor constantly their cyber environments in order to protect vital assets. Process mining may be a highly complementary and valuable part of an integrated cyber-security solution--reducing risk at scale for financial corporations and other sector stakeholders.

Process mining connects disparate cyber attack vectors and surfaces non-intuitive algorithmic process models of hostile processes from petabytes of cyber security attack logs and other sources of activity, which may be derived creatively. Machine-readable process diagrams provide data-driven inputs into simulations which enhance decision-making for leaders and gains advantage with predictive analytics of future hostile activity. In such a way, process mining enables actionable near-real time insights.



Anticipatory Defense: Modeling Cyber Attack Processes

- Denial-of-service (DoS)
- Distributed denial-of-service (DDoS)
- Man-in-the-middle (MitM)
- Phishing and spear phishing
- Drive-by
- Password attack.
- Cross-site scripting (XSS)
- Eavesdropping

Need

- Defend against cyber threats
- Decrease opportunities for surprise
- Improve knowledge of emerging threats
- Automate analysis
- Fuse data from non-traditional sources
- Temporal/spatial coverage
- Near Real-time

Technology

- Process mining/analytics
- AI/ML with hidden Markov models (HMM)
- Platform agnostic
- Derive time stamped events
- Peta-byte scalable

Benefits

- Algorithmic bad actor process models
- Simulate future scenarios
- Reduce risk
- Improve decision-making
- Anticipatory/predict future activity

© 2019 Copyright More Cowbell Unlimited, Inc.

A Brief Introduction to Reflexive Control and Information Warfare

Reflexive Control (RC) Theory has origins in Russia as early as the 1930s. The technique combines models of enemy decision-making processes with targeted information campaigns designed to exploit human-mental or computer-based decision-making process weaknesses (Thomas 2004). Information introduced into processes inclines the adversary toward taking an action that favors the attacker. This information need not be false; it may also be true or half-true information.

The information age presents new and vivid challenges relating to information warfare. False, irrelevant, altered, untimely, and/or overwhelming information may significantly slow or cripple critical information infrastructures. RC is being adapted into the cyber domain and being deployed against automated data-processing systems which contain significant decision-making processes.

Novel, scalable process-oriented methodologies augment cyber security efforts by offering a data-driven lens to understand financial services sector critical infrastructure processes.

Red Team: Cyber Security Process-related Vulnerabilities

"Red Team" projects are intensive self-examinations from an adversary's perspective and are a well-known technique to build up defensive capabilities by having friendly forces simulate enemy tactics to discover weaknesses (Zenko 2015).

Many types of log data can be mined by Red Team cyber security analysts, perhaps starting with the stipulation that the attacking Red Team has an internal mole providing logs, providing both insights into the human operations of a target (a corporation, for example) and machine decision making processes.

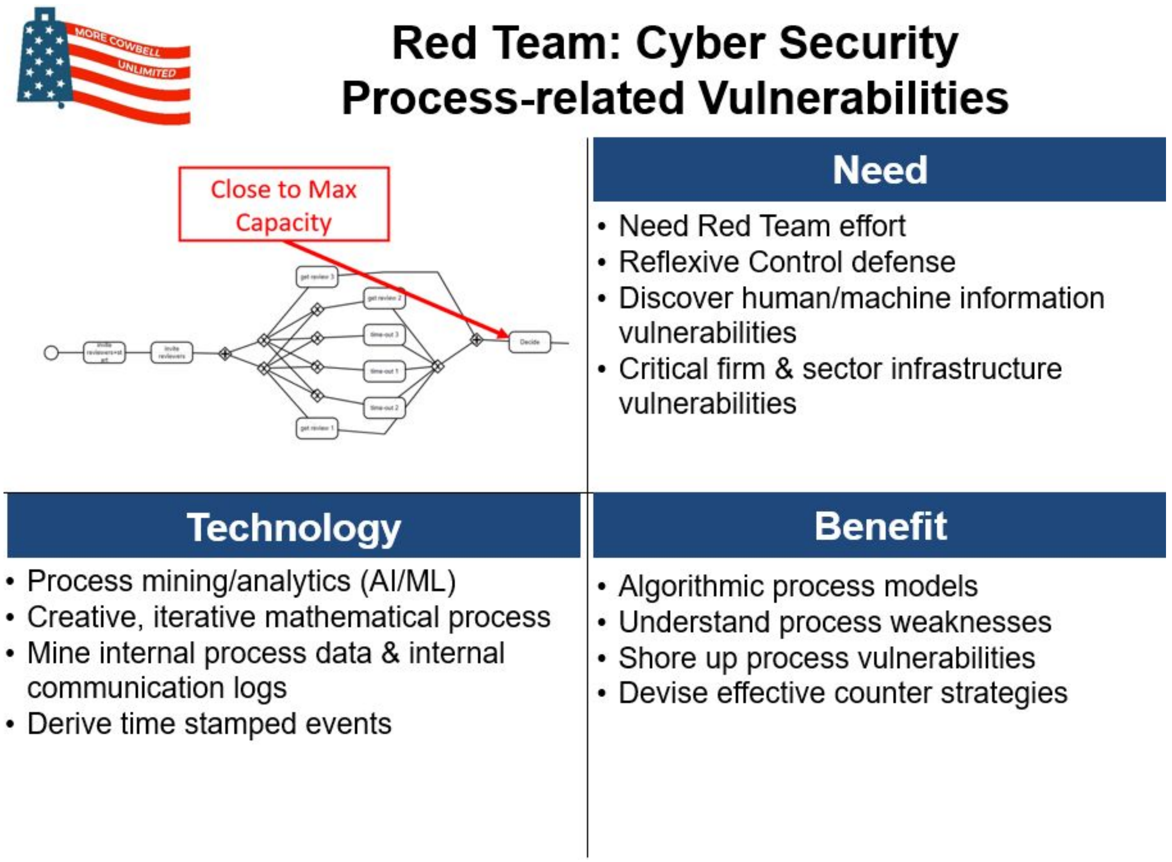
Analysts may employ process mining algorithms and get a process map which illuminates vulnerabilities--enabling analyses in the context of infrastructure information operations. This methodology may potentially be automated and scaled defensively across the entire financial critical infrastructure sector. For example, process nodes which are at or near capacity are at risk for targeted information overwhelm tactics, which can cripple a firm's operations.

Cybersecurity, in particular, is an area where both Red Team and event log collection strategies are well-known (Diogenes and Ozkaya 2018), the latter being especially ripe for process mining technologies (Huynh and Le 2012). One immediate application for process mining in cybersecurity applications is thus for Red Teams to mine target (internally available) log data in preparation for attacks. To the authors' knowledge, this low-hanging cybersecurity strategy is rarely mentioned in textbooks--even when Red Team techniques and (computer) process log monitoring techniques are mentioned side-by-side.

Red Teams could also feign a series of attacks or otherwise provoke the adversary (such as with noisy "kiddie scripts" or DDoS attacks in a cybersecurity context) and then mine the resulting mole-obtained email messages to learn the enemy's response patterns. (Enemy-obtained email messages with follow-on RC effects have been the subject of much recent press coverage, and thus a legitimate Red Team anti-RC starting assumption (2016 Democratic National Committee email leak 2019).) Valuable insights, such as typical alerting and response times, might be gleaned from process mining of adversarial responses to feigned attacks. Even if the adversary follows strict email-silence in discussing cyber security matters, email or other communications logs might still detect adversarial responses in

© 2019 Copyright More Cowbell Unlimited, Inc.

the form of canceled meetings or other unusual activity patterns that could provide insights into otherwise hidden attack detection and response by the adversary.



Red Team: Cyber Security Process-related Vulnerabilities

Need

- Need Red Team effort
- Reflexive Control defense
- Discover human/machine information vulnerabilities
- Critical firm & sector infrastructure vulnerabilities

Technology

- Process mining/analytics (AI/ML)
- Creative, iterative mathematical process
- Mine internal process data & internal communication logs
- Derive time stamped events

Benefit

- Algorithmic process models
- Understand process weaknesses
- Shore up process vulnerabilities
- Devise effective counter strategies

Defending Financial Markets

Understanding financial markets through a process lens would be very useful to help steel this infrastructure from RC or information warfare attacks. The 2008 financial crisis prompted DoD to sponsor wargames simulating an adversarial attack on financial markets (Javers 2009). Regulatory agencies also responded to the financial crisis by further increasing the already vast amounts of data collected from firms (FINRA 2010).

Regulatory agencies like FINRA process enormous amounts of data each day (Chen 2018; FINRA 2018b) to provide "market surveillance" to mitigate and simulate financial risks (Cook 2017; FINRA 2018a) including risks to national security. This market process surveillance can help the United States understand process vulnerabilities which are susceptible to cyber RC attack (as well as facilitate regulatory agency's normal attempts at understanding the behavior of market participants).

BPMN models discovered from process mining come baked with descriptive statistics, transition probabilities, and capacity estimates. These data allow financial services stakeholders to quickly understand process-related vulnerabilities. Vast daily regulatory filing data (Chen 2018; FINRA 2018b) should provide more than sufficient data for process mining to help both regulators and national security agencies protect the nation's financial markets.

© 2019 Copyright More Cowbell Unlimited, Inc.

Bibliography

"2016 Democratic National Committee Email Leak." 2019. *Wikipedia*. https://en.wikipedia.org/w/index.php?title=2016_Democratic_National_Committee_email_leak&oldid=884606265 (February 22, 2019).

Bicknell, John W, and Werner G Krebs. 2019. "Process Mining: The Missing Piece in Information Warfare." : 25.

Chen, James. 2018. "Order Audit Trail System - OATS." *Investopedia*. https://www.investopedia.com/terms/o/order_audit_trail_system.asp (February 20, 2019).

Cook, Robert. 2017. "Equity Market Surveillance Today and the Path Ahead | FINRA.Org." https://www.finra.org/newsroom/speeches/092017-equity-market-surveillance-today-and-path-ahead (February 20, 2019).

"Critical Infrastructure Sectors." 2013. *Department of Homeland Security*. https://www.dhs.gov/cisa/critical-infrastructure-sectors (February 25, 2019).

Diogenes, Yuri, and Erdal Ozkaya. 2018. *Cybersecurity – Attack and Defense Strategies: Infrastructure Security with Red Team and Blue Team Tactics*. Birmingham, UK: Packt Publishing.

"Financial Services Sector-Specific Plan." 2015. : 28.

FINRA. 2010. "SR-FINRA-2010-044 | FINRA.Org." http://www.finra.org/industry/rule-filings/sr-finra-2010-044 (February 20, 2019).

———. 2018a. 13 *13: How the Cloud and Machine Learning Have Transformed Market Surveillance | Episode 13*. https://embed.simplecast.com/d203ed4a?color=f5f5f5 (February 20, 2019).

———. 2018b. "FINRA Handles Record Volume of Market Activity through First Six Months of 2018 | FINRA.Org." http://www.finra.org/newsroom/2018/finra-handles-record-volume-market-activity-through-first-six-months-2018 (February 20, 2019).

Huynh, Viet H., and An N. T. Le. 2012. "Process Mining and Security: Visualization in Database Intrusion Detection." In *Intelligence and Security Informatics*, Lecture Notes in Computer Science, eds. Michael Chau, G. Alan Wang, Wei Thoo Yue, and Hsinchun Chen. Springer Berlin Heidelberg, 81–95. https://www.researchgate.net/publication/291583989_Process_Mining_and_Security_Visualization_in_Database_Intrusion_Detection.

Javers, Eamon. 2009. "Pentagon Preps for Economic Warfare." *POLITICO*. https://www.politico.com/news/stories/0409/21053.html (February 20, 2019).

Thomas, Timothy. 2004. "Russia's Reflexive Control Theory and the Military." *The Journal of Slavic Military Studies* 17(2): 237–56.

Zenko, Micah. 2015. *Red Team: How to Succeed By Thinking Like the Enemy*. 1 edition. New York: Basic Books.

© 2019 Copyright More Cowbell Unlimited, Inc.