## Call for Contributions for

**Submission:**

**1. Inform the Chair:** with the Title of your Contribution

**2. Submission URL:**

**https://www.iariasubmit.org/conferences/submit/newcontribution.php?event=CYBER+2018+Special**

Please select Track Preference as **CAS-IAADR + CCAML**

Special track

# CAS-IAADR + CCAML: Cyber Attack Surfaces and the Interoperability of Architectural Application Domain Resiliency (CAS-IAADR) via Cyber Characterization, Analytics, and Machine Learning (CCAML)

**Chair and Organizer**
Dr. Steve Chan, Decision Engineering Analysis Laboratory, USA
stevechan@alum.mit.edu

**Co-Chair and Organizer**
Dr. Tom Klemas, Decision Engineering Analysis Laboratory, USA
tklemas@alum.mit.edu

along with

CYBER 2018, The Third International Conference on Cyber-Technologies and Cyber-Systems
http://www.iaria.org/conferences2018/CYBER18.html
November 18 - 22, 2018 - Athens, Greece

Energy Managed Services are a type of managed service, which is the practice of outsourcing certain functional roles and responsibilities to enhance the involved operations and reduce expenses. A Managed Service Provider (MSP) is an outsourced third-party company that remotely manages and assumes responsibility for the involved operations. By leveraging available high-speed Internet connections and user-friendly Software-as-a-Service (SAAS) interfaces, MSPs offer a pragmatic way to quickly scale (e.g., "pay-as-you-go") at a reasonable cost. Within the energy sector, various MSPs are helping building owners and operators lower energy use, increase building operations efficiency, and optimize the climate control conditions in the tenant working spaces). These MSPs leverage cloud-based software and the granular control of Internet of Things (IOT) devices to deliver their managed services. This paradigm segues to the attack surface problem at the "weak link in the chain" (which represents the weakest member of a system and because of this point of failure, the entire system may fail). We can define attack surface as the exposure or exploitable vulnerabilities that exist within a system. The three most common attack surfaces include: (1) human attack surface (e.g. social engineering, insider threat, errors of omission or commission), (2) network attack surface (e.g., open ports on outward facing web servers, code listening on those ports, and services available on the inside of the firewall), and (3) software attack surface (with a focus on web applications).

Putting aside the large issue of human attack surfaces, the amalgam of network attack surfaces and software attack surfaces constitute high exposure dimensions. According to the SANS Technology Institute, Teredo tunnels (which is a protocol that provides Internet Protocol version 6 (IPv6) connectivity for IPv6-capable hosts that are on Internet Protocol version 4 (IPv4), but that do not have a native connection to an IPv6 network) may allow attackers to bypass IPV4 devices, such as firewalls and intrusion detection systems (IDS), which are not Teredo-aware. In many cases, there exist network tunnels, such as secure shell (SSH), Point-to-Point Protocol (PPP) and Virtual Private Networks (VPNs). The basic idea behind network tunnels is that non-routable data packets maybe encapsulated inside routable data packets for transmission over the Internet; at the destination, the encapsulation will be removed, and the original data will enter the private network, as if it had stemmed locally. The security dilemma is that it is very difficult to know what is running inside of these network tunnels; consequently, network tunnels represent a network attack surface that attackers can covertly exploit.

Proceeding on to software attack surfaces, an ever-increasing amount of funding is being spent on developing an escalating number of web applications that are mission-critical. Concurrently, attackers are becoming more adept at exploiting web applications. There are indeed penetration testing (a.k.a. pen testing) tools and web application security assessment tools that help identify known and unknown vulnerabilities. These tools can assist in: (1) reducing the amount of code executing (i.e. turning off certain features), (2) reducing the volume of code that is accessible to users (i.e. establishing user privileges), (3) constraining the damage, if code is indeed exploited (i.e. damage control rule sets). However, there are limitations to these prototypical tools. Pen testing itself is limited in scope, and most organization are not able to exhaustively test the entire portfolio of systems due to resource constraints and practicality. Also, while pen testing involves a certain set of tests over a certain amount of time; yet attackers can plan and execute over a longer time frame. Furthermore, pen testing is limited to the models that are created, and the attack surface might be at higher exposure than anticipated. There are also limitations to the automated tools for web application security scanning. While scanners can identify the more serious technical flaws within applications, they are not able to identify logical (e.g., architectural, design) flaws that were introduced before the coding, authentication, and authorization took place.

Shockingly, one of the points of failure within the Energy Sector (which involves systems that support critical infrastructural elements) is the mission-critical web applications used by Energy Managed Service Providers. Despite the mission critical aspect of the energy domain, many of the lessons learned from the design vulnerabilities of the application domain of web application software have not yet been fully applied to the energy domain. Injections and man-in-the-middle attacks are well-known. Configuration alterations are also prevalent, and these and other attack forms need to be more robustly addressed. There are also the vulnerabilities associated with the progress that has been made in the ecosystem of blockchain for the energy sector.

Since MSPs are often responsible for remotely managing end-point systems, they typically have direct, privileged access to their clients' networks. MSPs, particularly if they are also cloud or hosting providers, may also house a large amount of client data (often sensitive or confidential) on their own internal infrastructure. According to PricewaterhouseCoopers (PwC), one of the largest sustained global cyber campaigns, Operation Cloud Hopper, has been targeting managed MSPs so as to gain access to the diverse MSP client networks. Targeting just one MSP can give an attacker access to a large number of different organizations. According to PwC, the industries targeted include energy. Consequently, to provide more robust cyber resiliency, we examine the common design vulnerabilities and architectural enhancements that may be applied across the cyber attack surfaces of various domains to enhance resiliency and then posit analytics that can provide insight into logical (e.g. architectural, design) flaws.

**Topics include, but not limited to:**

- Teredo Vulnerabilities (e.g., static, embedded SSH keys)
- Domain Name System (DNS) Vulnerabilities (e.g., cache poisoning)
- Logical Flaws (i.e., beyond technical flaws)
- Cyber characterization, analytics, and machine learning (CCAML) (an exploration of the convergence of cyber analytics, machine learning, and characterization approaches to improve cyber security operations)

**Important Datelines**

Inform the Chair: As soon as you decided to contribute

Submission; ~~August 1~~ October 5
Notification: ~~September 1~~ October 20
Registration: ~~September 15~~ October 30
Camera-ready: ~~September 25~~ October 30
***Note:*** *These deadlines are somewhat flexible, providing arrangements are made ahead of time with the chair.*

**Contribution Types**

- Regular papers [in the proceedings, digital library]
- Short papers (work in progress) [in the proceedings, digital library]
- Posters: two pages [in the proceedings, digital library]
- Posters: slide only [slide-deck posted on www.iaria.org]
- Presentations: slide only [slide-deck posted on www.iaria.org]
- Demos: two pages [posted on www.iaria.org]

**Paper Format**

- See: http://www.iaria.org/format.html
- Before submission, please check and comply with the editorial rules: http://www.iaria.org/editorialrules.html

**Publications**

- Extended versions of selected papers will be published in IARIA Journals: http://www.iariajournals.org
- Print proceedings will be available via Curran Associates, Inc.: http://www.proceedings.com/9769.html
- Articles will be archived in the free access ThinkMind Digital Library: http://www.thinkmind.org

**Paper Submission**

**https://www.iariasubmit.org/conferences/submit/newcontribution.php?event=CYBER+2018+Special**
Please select Track Preference as **CAS-IAADR + CCAML**

**Registration**

- Each accepted paper needs at least one full registration, before the camera-ready manuscript can be included in the proceedings.
- Registration fees are available at http://www.iaria.org/registration.html

**Contacts**

Steve Chan: stevechan@alum.mit.edu
Tom Klemas: tklemas@alum.mit.edu
CYBER Logistics: steve@iaria.org
-------------------------