International Association of Drilling Contractors

Cybersecurity Committee
11 Oct 2018
IADC
3657 Briarpark Drive, Suite 200
Houston, TX 77042

Attendance

Name		Company Name
Jose	Brana	**Weatherford**
Eric	Dila	**Noble Drilling**
Stewart	Gillies	**Aberdeen Drilling Consultants**
Sean	Gray	**Stena Drilling**
Siv Hilde	Houmb	**SECURE-NOK**
Larry	Humes	**Noble Drilling**
Britt	John	**Mission Secure**
Jeff	Johnsen	**ExxonMobile**
Thomas	Koithan	**Weatherford**
Francis	Lobo	**Canopius**
Del	Manning	**Rowan Companies**
Melissa	Mejias	**IADC**
Felipe	Mondragon	**Noble Drilling**
Juan	Negrete	**Rowan Companies**
Ben	Ramduny	**Seadrill**
Mike	Reynolds	**Pacific Drilling**
Matthew	Romero	**ABS**
Brady	Rustin	**Lloyds Regisitry**
Nathan	Singleton	**Helmerich & Payne International Drilling**
Sandy	Smith	**Rowan Companies**

International Association of Drilling Contractors

Agenda for the meeting:

1. Welcome and Introductions

2. Review of Antitrust Guidelines and Facility Orientation

3. Review of Minutes from Last Meeting

4. Update on Legislative and Standardization Activities

5. IADC Cybersecurity Guidelines Development – Network Segmentation

6. AOB and Close of Meeting

Minutes:
1. Welcome, facilities orientation, safety moment, and short introduction of the participants – "round around table".

2. Meeting delegates was reminded of the IADC antitrust guidelines.

3. Minutes from the committee meetings are posted at: http://www.iadc.org/cybersecurity-committee/meeting-minutes/. There were no comments to the minutes from the Aug 9, 2018, IADC Cybersecurity Committee meeting.

4. Update on Legislative and Standardization Activities by Melissa Mejias, IADC. Please see appendix to the minutes.

5. IADC Cybersecurity Guidelines Development – Network Segmentation by Ben Ramduny, Co-Chair. The guidelines are about 60% completed. Thus far, the focus has been on standards and best practices for network segmentation, IEC 62443 with identification of zones and conduits, and networking protocols, especially identifying whether the various protocols in use are routable or not (e.g. serial). The sections that still needs to be written are guidance regarding how to define a risk-based network segmentation strategy for a drilling asset and from this strategy, identify critical components and define requirements for segmenting the network. The latter should be based on the needs related to protecting critical components in a manner that achieves HSE, business continuity and financial goals. This part should also include an example. The below figure shows an outline of the network segmentation guidelines and the status (as per Oct 11) of each section.

The meeting agreed to setup dedicated review and working sessions between this meeting and the next committee meeting Dec 13, 2018. The co-chairs: Ben Ramduny and Juan Negrete, will organize these sessions and reach out to the meeting participants to solicit volunteers to help with the various sections. Please consider contributing to this work. Many thanks.

Action Point: Ben Ramduny and Juan Negrete to reach out to the meeting participants and organize a set of review and working sessions in October and November. The goal is to have the network segmentation guidelines in the first complete draft state at the Dec 13, 2018, committee meeting.

International Association of Drilling Contractors

#	Title	Section Objective	Action required	Author
	Introduction and Background		Review	
1	Standards and Best Practices for Network Segmentation	Introduce next section	Review & Update	
1.1	ISA/IEC 62443 Overview and Application to Drilling Asset	Review the standard and provide a narrative on how the standard could be applied to a MODU	Review & Update	
1.2	ISO 27001/2 Overview and Application to Drilling Assets	Review the standard and provide a narrative on how the standard could be applied to a MODU	Review & Update	
1.3	NIST Overview and Application to Drilling Assets	Review the standard and provide a narrative on how the standard could be applied to a MODU	Review	
1.4	Defining a Network Segmentation Strategy based on Risk	Guidance on how to ensure that a segmentation project is segmenting the network because of risks to the components within the segment	Write Section	
2	Guidelines for Identifying relevant network Segments	Introduce next section	Review	
2.1	Identifying the Criticality of Components	Guidance on how assess each component and determine how critical it is to the drilling operation a safety o the MODU	Write Section	
2.2	Identifying Remote and 3rd Party Connections		Write Section	
2.3	Defining the limitations and requirements of each Network Segment	Guidance on how determine when segmentation may not be possible to process or technology constraints	Write Section	
3	Designing Network Segmentations and Remote Access		Write Section	
4	Guidelines for Controlling Traffic Flows Between Network Segments	Introduce next section	Review	
4.1	Uni-Directional or Bi-Directional Traffic Flows	Guidance on possible traffic flow control mechanisms based on whether the communication is 1 way or both ways	Review	
4.1	Selecting traffic flow control mechanisms	Guidance on choosing appropriate traffic flow control mechanisms	Review	
5	Practical Guidelines for Implementing Network Segmentation	Guidance on options that can help to reduce risk if full segmentation is not possible due to technical constraints or budget.	Review	
6	Example (applying the guidelines to a generic 6th gen drillship	A step by step example of how to apply the guidelines to an existing MODU	Review & Update	
7	Maintaining Accurate Network Architecture Designs	Guidance on how to build a process to ensure that network diagrams are maintained and remain current	Review & Update	
8	Periodic Auditing of network Segmentation design and policies	Guidance on what should be periodically reviewed and the frequency to ensure that the segmentation deployed on day 1 remains effective on day x following numerous operation changes.	Write Section	
9	Conclusions	Summary and reference to further reading	Review	

6. AOB and close of meeting. The committee meetings are announced on the IADC website. Please remember to register. The next committee meeting is December 13 in Houston, TX. This committee meeting will be organized as a full-day workshop hosted by BP. The workshop will be organized as a red team and blue team tabletop exercise. The workshop participants will be divided into groups who in turn will act as attackers and then as responders. The attack targets will be two types of drilling assets: one land and one offshore. The attack scenarios will focus on malware/virus entering into the control system from email, USB, and vendor update. The attack scenarios will need to be detailed to a level where each step in the attack is described, so that the attack can be played out step-by-step at the workshop. The following action points were defined for the attack scenario development.

==Action Point: Nathan Singleton, Matthew Romero, and Siv Hilde Houmb are responsible for developing the attack scenarios for the land drilling rig.==

==Action Point: Ben Ramduny, Juan Negrete, Eric Dila, and Mike Reynolds are responsible for developing the attack scenarios for the offshore drilling rig.==

==Action Point: Siv Hilde Houmb will coordinate with the two groups to ensure that the attack scenarios are in a suitable form for the workshop.==

Updated and tentative schedule of deliverables for the IADC Cybersecurity Committee:
- December 2018 – Guidelines for Network Segmentation.
- December 2018 – Cybersecurity Training v1.0.
- June 2019 – Guidelines for Hardening of Control Systems.
- June 2019 – Guidelines on Security Monitoring and Audit.

There were no other business and meeting adjourned.

Appendix:
1. [Update on Legislative and Standardization Activities](#).