Threat Modeling for System of Systems

Nataliya Shevchenko

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM21-0213

Agenda

Why Threat Modeling? (Study Cases)
What is Threat Modeling?
Types of Attacks
Threat Modeling Methods
- STRIDE
- Attack Tree
- PASTA

Evaluation Criteria
Threat Modeling in SDLC
Threat Modeling in Agile
Threat Modeling in DevOps
Case Studies: Review
Q&A

2019: Norsk Hydro Attack, Norway - 1

- In March 2019, Norsk Hydro was hit with the LockerGoga ransomware attack, which compromised the company's IT systems. The outage was felt globally at Norsk's facilities and severely impacted the company's ability to produce its rolled aluminum products. The company didn't pay the attackers, but still suffered a $52M loss.

Source: https://www.computing.co.uk/ctg/news/3074971/norsk-hydro-cyber-attack-cost
Source: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware/

2019: Norsk Hydro Attack, Norway - 2

- “[T]he ransomware was dropped and executed by a renamed PsExec tool…. This could mean that the **network was already compromised**, and that the attackers **conducted lateral movement**. Since PsExec requires credentials to work, the attackers may have already obtained the credentials either through **brute force, spearphishing, or a previous malware infection or attack**.”
- Production was done manually, but recovery took months

Source: https://www.computing.co.uk/ctg/news/3074971/norsk-hydro-cyber-attack-cost
Source: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware/

2017: Attack on Power Grid, USA - 1

- "[T]he hackers went after the system's **unprotected underbelly**.… From these tiny footholds, the hackers worked their way up to **the supply chain**."
- "The scheme's success came [from] … how it **exploited trusted** business **relationships** using impersonation and trickery."
- "Some companies were unaware they had been compromised until government investigators came calling, and others didn't know they had been targeted until contacted by the *Journal*."

Source: https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112

2017: Attack on Power Grid, USA - 2

- ICS cybersecurity chief for Homeland Security said that the hackers “had **penetrated the control-system area** of utilities through poorly protected jump boxes.* The attackers had legitimate access, the same as a technician” … could have temporarily **knocked out power**.
- Industry experts say the state sponsored hackers “likely **remain inside some systems**, undetected and awaiting further orders.”

* “jump box” – a computer that give technicians a way to move between the two systems.

Source: https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112

2020: SolarWinds Attack, USA, UK, … - 1

- A sophisticated hacking group **backed by a foreign government** stole information from the U.S. Treasury Department and a U.S. agency … ”
- “A sophisticated malware campaign attributed to Russian intelligence goes beyond a **tainted software update** from IT monitoring company SolarWinds ...”
- “The hackers used a variety of legitimate software and **cloud hosting services** to access the systems of nine federal agencies and 100 private companies.”

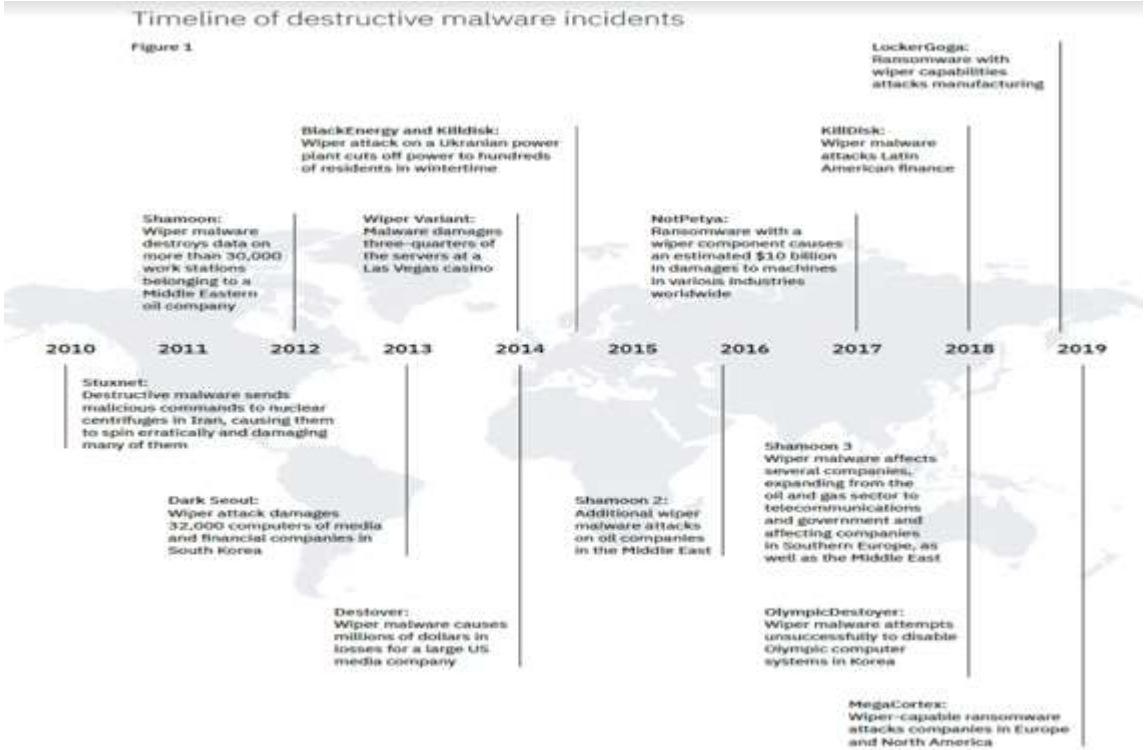
Source: https://www.reuters.com/article/usa-cyber-treasury-idUSL1N2IT0I8; https://www.cnet.com/news/solarwinds-not-the-only-company-used-to-hack-targets-tech-execs-say-at-hearing/

2020: SolarWinds Attack, USA, UK, … - 2

- “Hackers managed to **access a system** that SolarWinds uses to put together **updates to its Orion product.”**
- Some hackers “gained entry to Microsoft services running on Malwarebytes' systems by **abusing third party apps with privileged access** to Office 365 and Azure products”.
- “[H]ackers used Amazon Web Services **cloud hosting** to run programs that **communicated with and controlled the malicious code** they installed on victimized systems. ”

Source: https://www.reuters.com/article/usa-cyber-treasury-idUSL1N2IT0I8; https://www.cnet.com/news/solarwinds-not-the-only-company-used-to-hack-targets-tech-execs-say-at-hearing/

Cyber Attacks Against Industrial Targets



Source: https://www.zdnet.com/article/cyberattacks-against-industrial-targets-double-over-the-last-6-months/

What is Threat Modeling? - 1

"Threat modeling is a process by which potential threats, such as structural vulnerabilities can be identified, enumerated, and prioritized—all from a hypothetical attacker's point of view. The purpose of threat modeling is to provide defenders with a systematic analysis of the probable attacker's profile, the most likely attack vectors, and the assets most desired by an attacker." *

*Wikipedia contributors. "Threat model." Wikipedia, The Free Encyclopedia. Wikipedia, The Free Encyclopedia, 22 May. 2019. Web. 19 Aug. 2019.

What is Threat Modeling? - 2

Asset - a resource of value, or something that an attacker wants to access, control, or destroy
Threat - a potential occurrence of an event or events that might damage or compromise an asset or objective
Vulnerability - a weakness in some aspect or feature of a system that makes an exploit possible
Attack - an action taken that utilizes one or more vulnerabilities to realize a threat to compromise or damage an asset

Basic TMM Idea

4-Step Framework

The four step framework provides a way to reason about the integration of TMM into the development process.

Source: Shostack, A. *Threat Modeling: Designing for Security.* Wiley, 2014. ISBN 978-1118809990.

Defender View vs. Attacker View

- Which assets to protect?
- What vulnerabilities to fix?
- How deep should cyber defense be?

Source: Shostack, A. *Threat Modeling: Designing for Security.* Wiley, 2014. ISBN 978-1118809990.

Types of Attacks

Spoofing (client, process, data flow)
Tampering (process, data flow, data store)
Repudiation (process, data store)
Information Disclosure (excavation, interception, elicitation)
Denial of Service (data flow, data store)
Elevation of Privilege (privilege abuse, authentication abuse and bypass)
Social Engineering Attack (spear-phishing, exploiting trust)
Supply Chain Attack (modification during manufacturing, manipulation during distribution)
Hardware Integrity Attack (hacking, malicious update)
Injection Attack (resource, code, traffic, object)
Obstruction Attack (route disabling, orbital jamming, physical destruction of component)

Source: CAPEC, MITER
Source: Shostack, A. Threat Modeling: Designing for Security. Wiley, 2014. ISBN 978-1118809990.

How to Model Threats

Identify the system's critical assets ("crown jewels").

Identify the system's trust boundaries.

Find system's vulnerabilities.

Identify ways the vulnerabilities can be exploited.

Profile potential attackers and their motives.

Identify attacker's goals and methods.

Calculate risks.

Identify mitigation strategies.

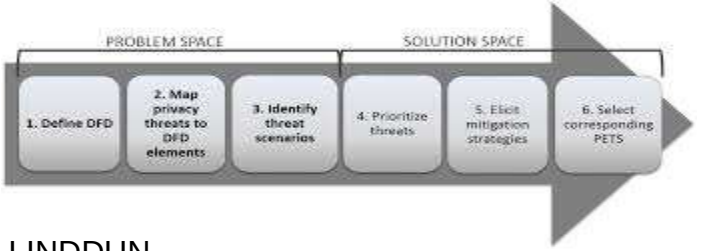
Threat Modeling Methods

P.A.S.T.A

STRIDE Threat Types

Desired Property	Threat	Definition
Authentication	Spoofing	Impersonating something or someone else
Integrity	Tampering	Modifying code or data without authorization
Non-repudiation	Repudiation	The ability to claim to have not performed some action against an application
Confidentiality	Information Disclosure	The exposure of information to unauthorized users
Availability	Denial of Service	The ability to deny or degrade a service to legitimate users
Authorization	Elevation of Privilege	The ability of a user to elevate their privileges with an application without authorization

Microsoft STRIDE Threat Types



LINDDUN

Denning, Friedman, Kohno
The Security Cards:
Security Threat Brainstorming Toolkit

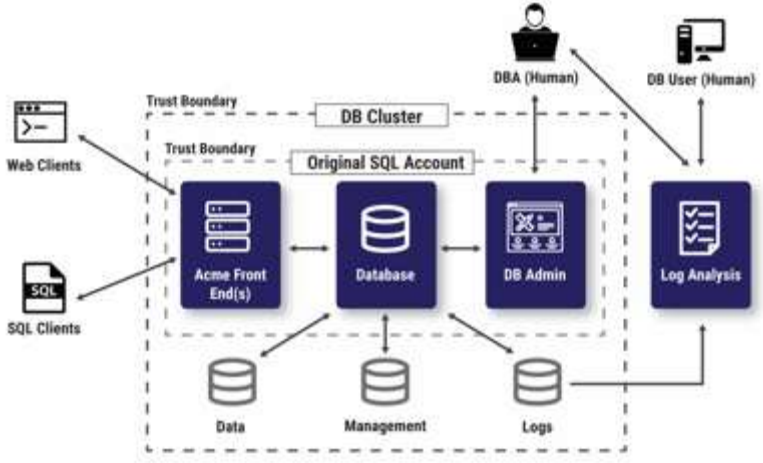
Jane Cleland-Huang's
Persona non Grata
http://www.infoq.com/articles/personae-non-gratae

Attack Tree

Threat Modeling Methods: STRIDE

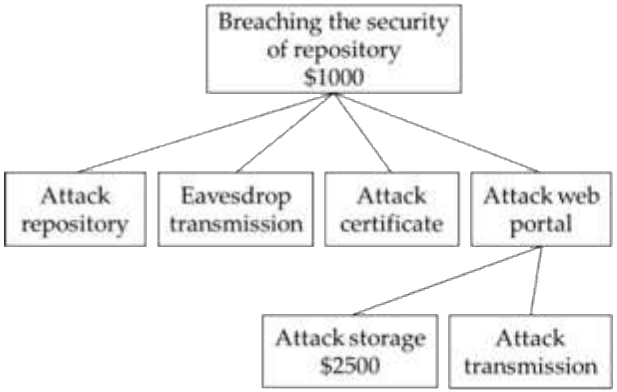
- Model the system: identify system entities, events, and boundaries of the system.
- Find threats: Answer the question *“what can go wrong with the system we’re working on”*
- Variants are STRIDE per Element, STRIDE per Interaction

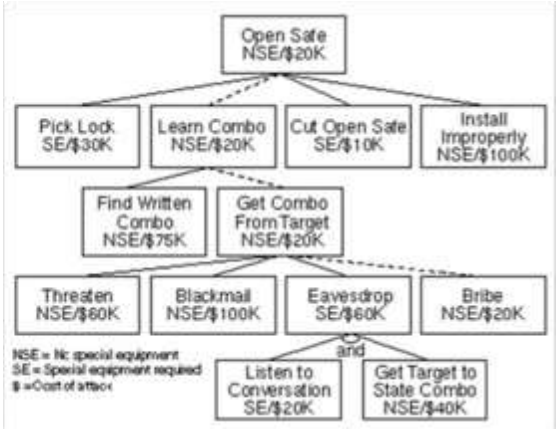
Threat	Property
Spoofing	Authenticity
Tampering	Integrity
Repudiation	Non-Repudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization



Threat Modeling Methods: Attack Tree

- Diagrams attacks on a system in tree form.
- The tree root - the goal for the attack.
- The leaves - ways to achieve the goal.
- Each goal is represented as a separate tree.





Threat Modeling Methods: PASTA

The Process for Attack Simulation and Threat Analysis (PASTA) is a seven-step, risk-centric methodology. It provides a seven-step process for aligning business objectives and technical requirements, taking into account compliance issues and business analysis.

- Easily extendable by additional methods
- Allow to approach from defender, attacker and system point of view
- Includes scoring and analysis

Methods Evaluation Criteria

Strengths and Weaknesses
- Maturity and usage
- Focus/perspective
- Time to implement
- Effectiveness
- Mitigation strategies

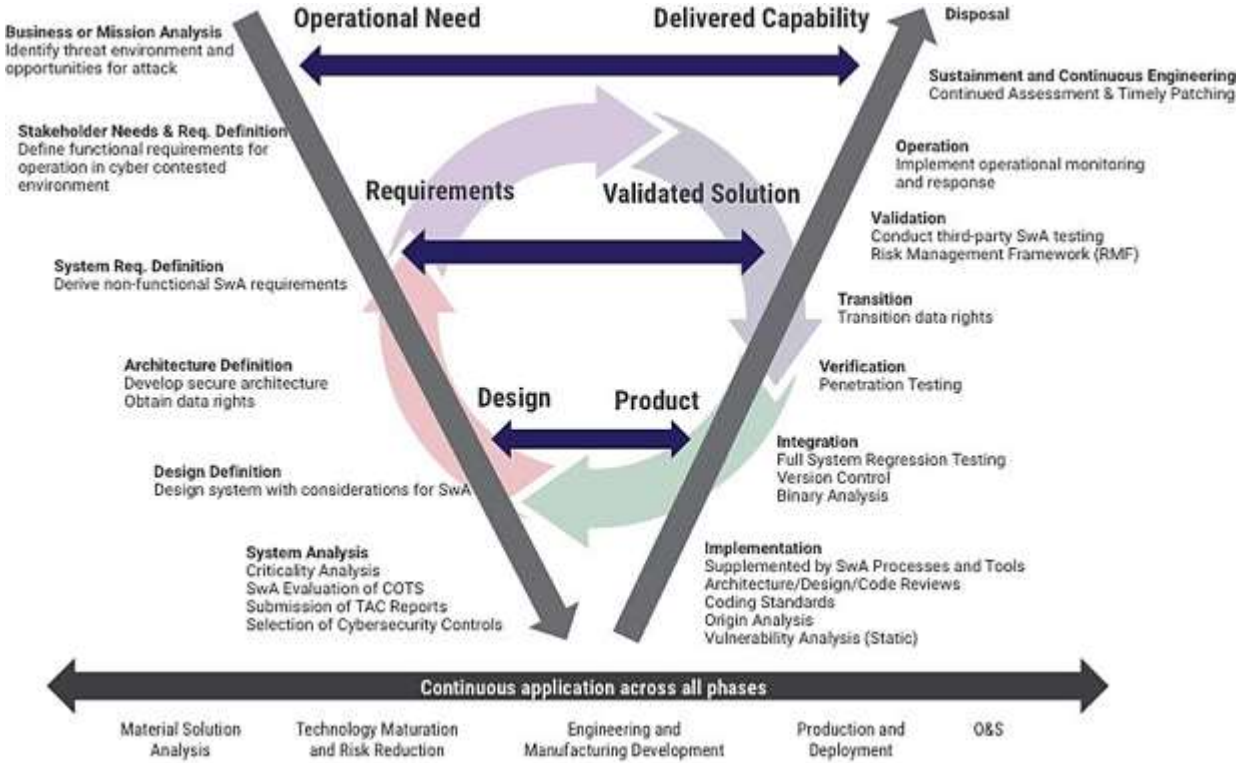
Adoptability
- Easy to use
- Easy to learn
- Documentation and support

Automation
- Availability of tools
- Integration options for tools into a SDLC
- Portability of tools

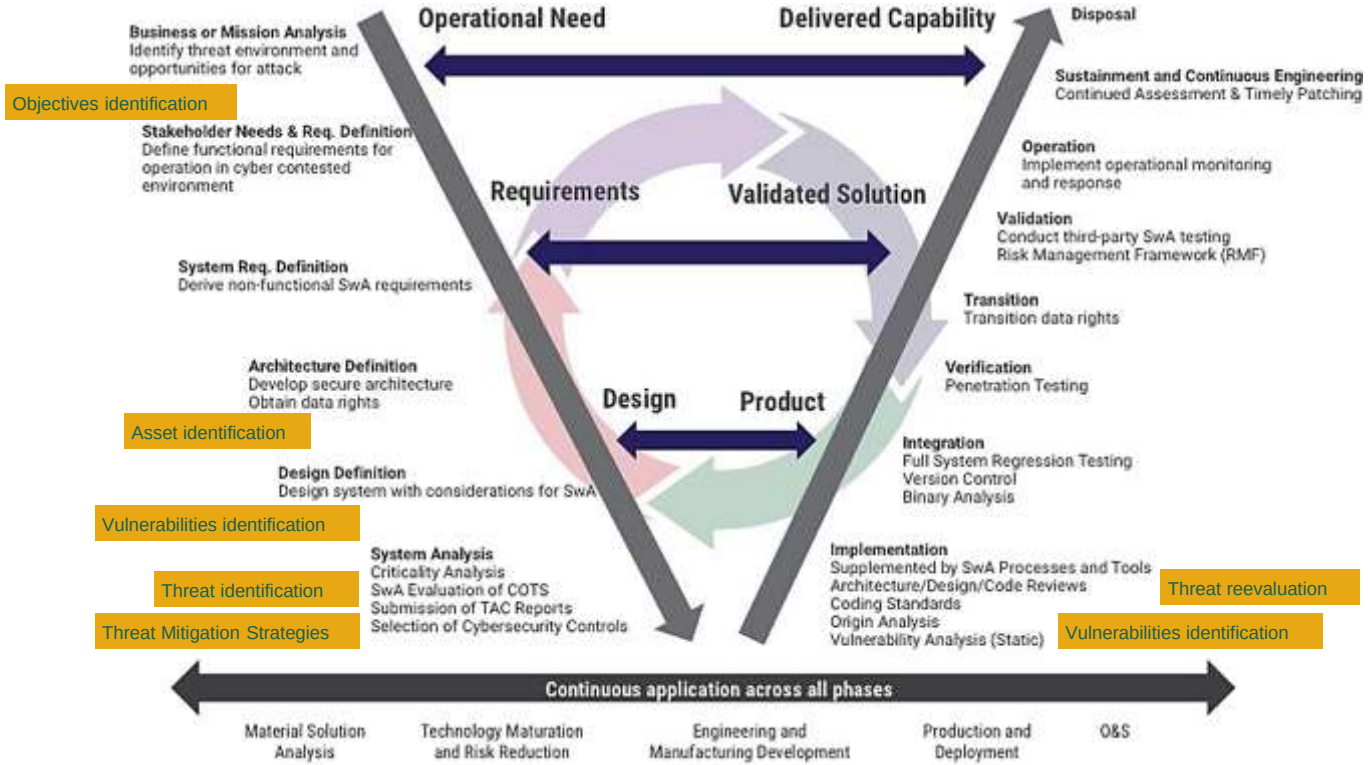
Tailorability
- Integration with SDLC
- Compatibility with Agile development process
- Scalability

Applicability to systems of systems
- Coverage of safety–security interdependency
- Integration of hardware and software threats

Tailorability

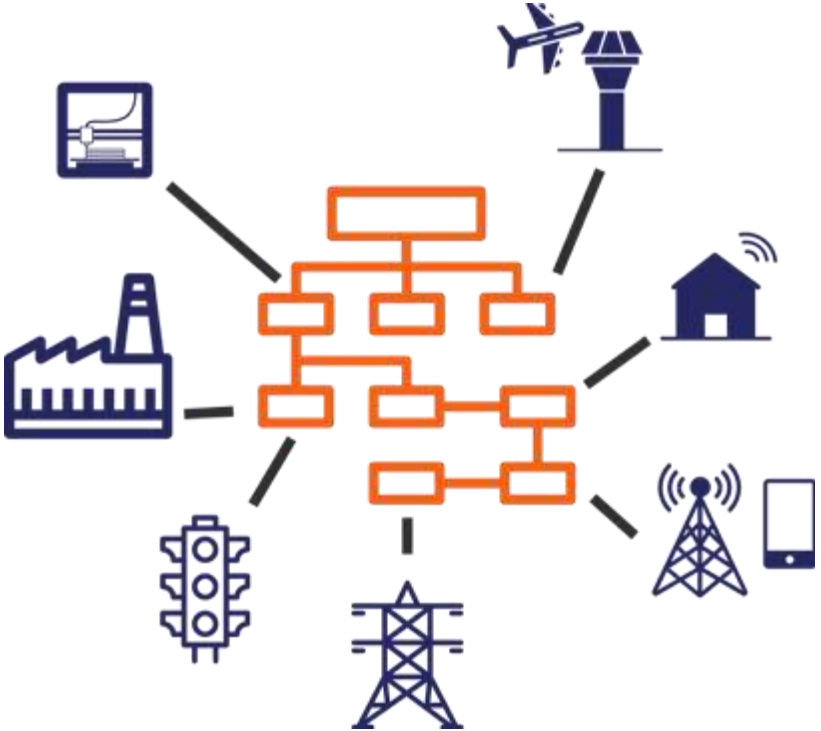


Threat Modeling in Software Development Life Cycle

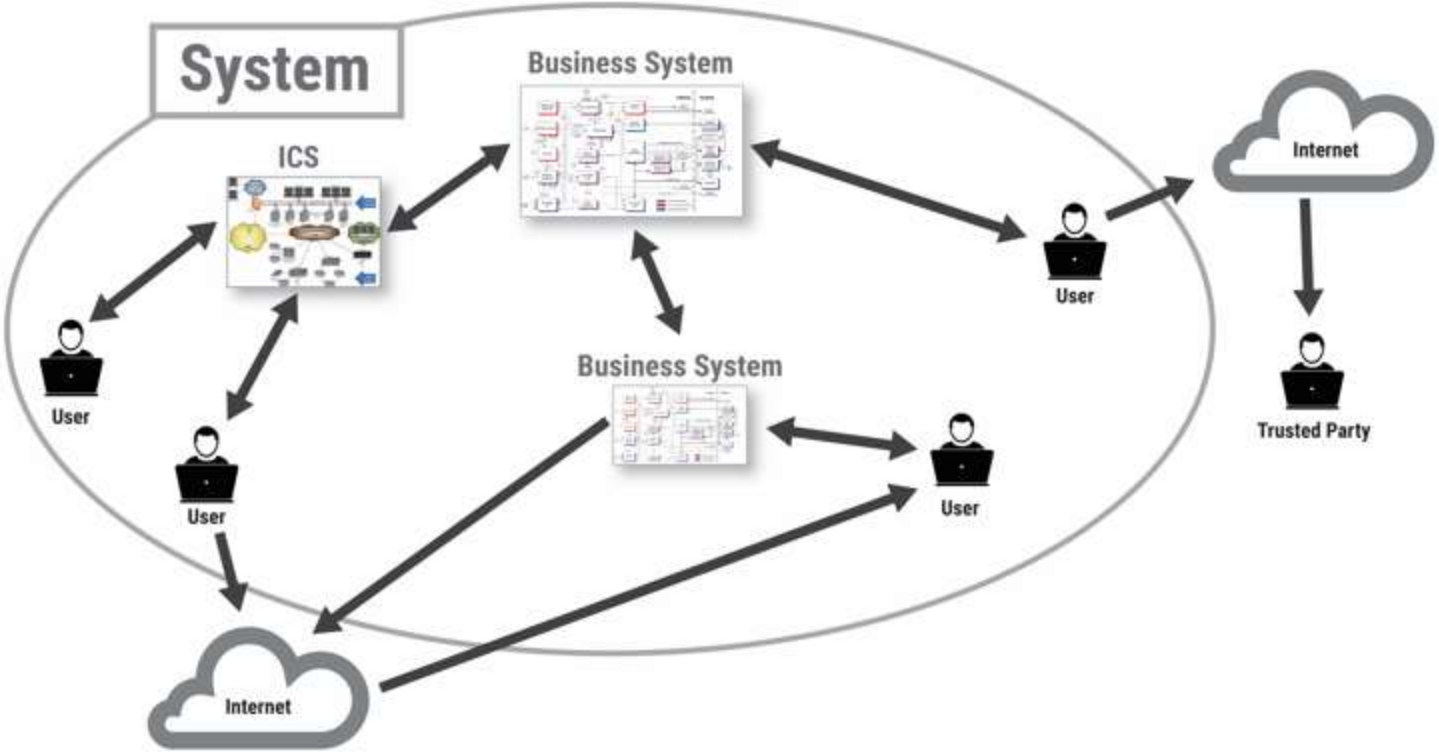


Applicability to Cyber-Physical Systems

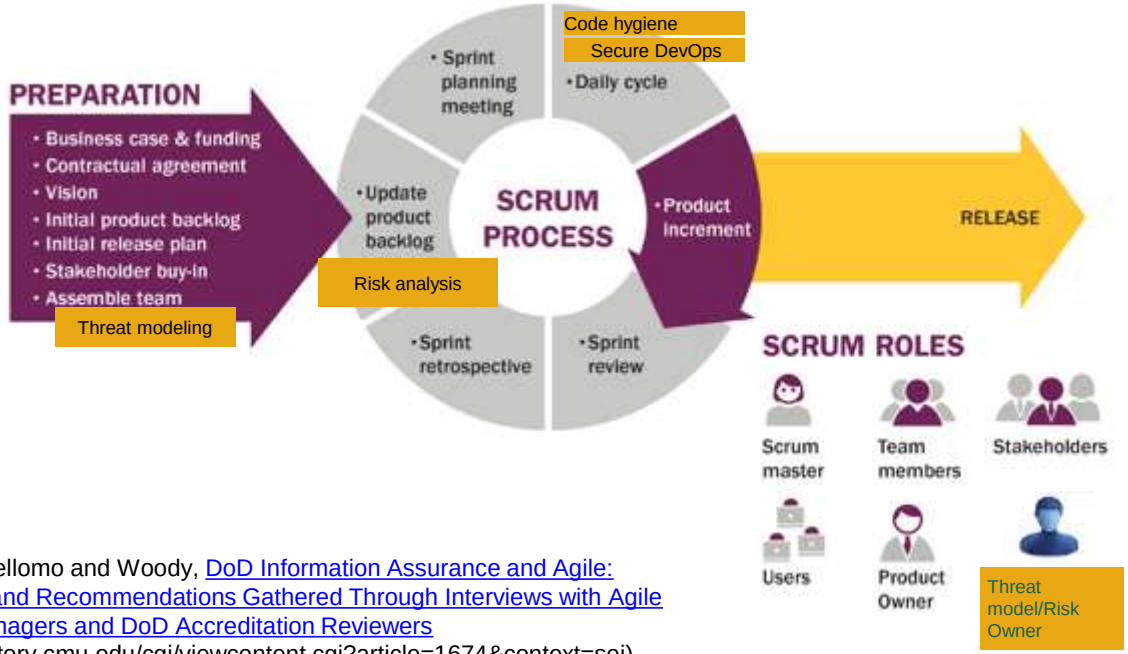
- Cellular, Automotive, Industrial, Aviation, Smart Grid, Embedded Medical
- Do the components in the physical systems support threat modeling efforts?
- Does the cyber-physical system have support equipment?
- What are the boundaries of the cyber-physical system, does it have a hidden boundary?
- Are there legacy concerns, long term support concerns?
- Safety is not Security



Applying to the System of Systems



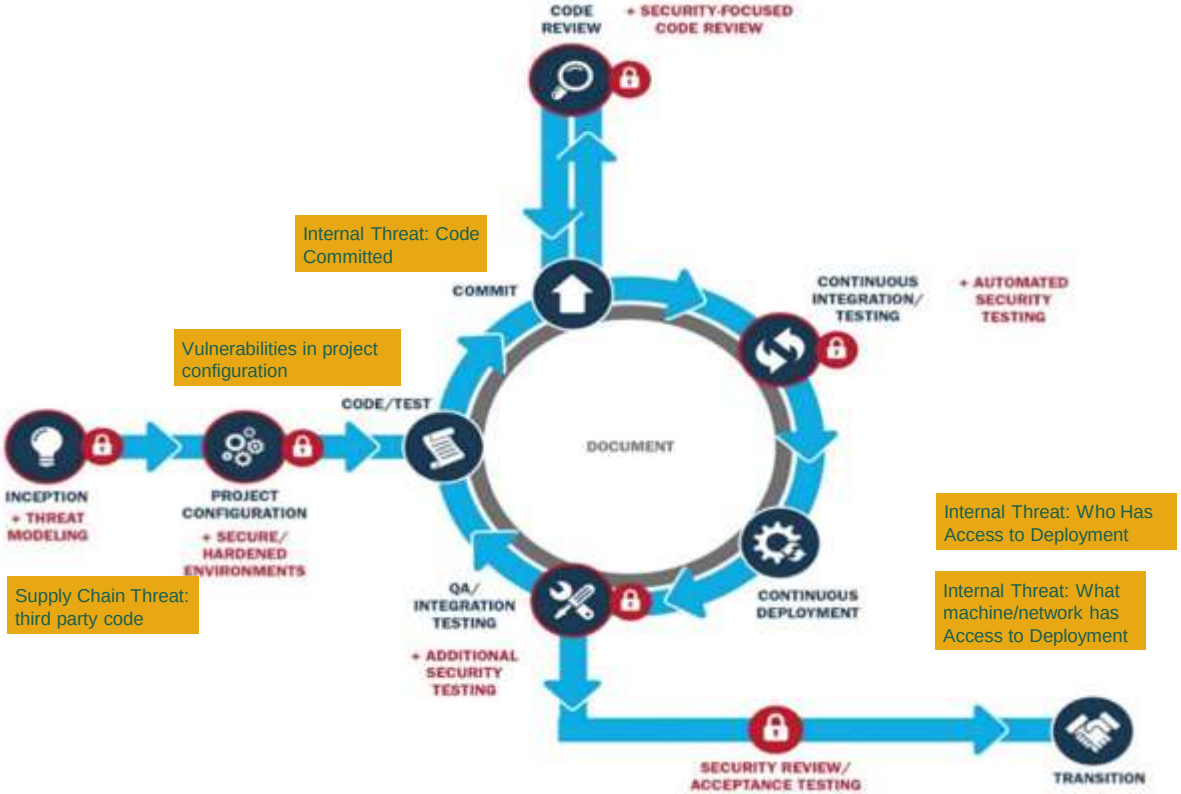
Threat Modeling in Agile



1. Code hygiene – introduce secure coding
2. Secure DevOps – include security tools
3. Threat modeling – represent a new role
4. Risk analysis – prioritize in backlog

(See also: Bellomo and Woody, DoD Information Assurance and Agile: Challenges and Recommendations Gathered Through Interviews with Agile Program Managers and DoD Accreditation Reviewers (http://repository.cmu.edu/cgi/viewcontent.cgi?article=1674&context=sei)

Threat Modeling in DevOps: System vs Pipeline



Case Studies: Review

Identify trust bounders
- Exposing Operational Technology systems to IT systems
- Poorly protected Business network connected to the internet
- Supply-chain issue

Identify “crown jewels” assets
- Critical ICS was on a network that was not air-gapped.
- Is air-gapped even possible anymore?

Human Factors
- Exploitation of trusted relationships
- Emails (spear-phishing)

Attack intent
- To take the ICS systems hostage
- To destroy the ICS systems

Threat Modeling Method

Questions