IEEE AUTOTESTCON 2022

August 29-September 1, 2022 ★ National Harbor, Maryland

Gaylord National Convention Center

PLEX

CYBERSECURITY ASSOCIATION OF MARYLAND, INC.

IEEE

ATC Cyber Panel Agenda

IEEE AUTOTESTCON 2022
August 29-September 1, 2022 • National Harbor, Maryland
Gaylord National Convention Center

AUTOTESTCON Cyber Panel discussions will include how Cyber Security best practices and policies relate to each of the four views, the effects each of the four views have on each other, and realistic Cyber Security implementation challenges ATS face today.

- Cyber Security 101; as it is today – Dave Sapp
- Cyber Attack Surface; an overview of ATS security control (Steve)
- The Human Element; users of ATS and their impacts (Connor)
- Supply Chain; sophisticated threat landscape (Diane)
- ATS Security Accreditation; what is the future? Jim Orlett

Please note that due to the sensitivity of the Cyber Security subject, these discussions will not delve into any specific details; either during the presentations or the responses to questions.

CYBER SECURITY
ASSOCIATION OF MARYLAND, INC.

Cyber Attack Surface

Steve Schink
Keysight Technologies Product Manager
LXI Consortium President

Cyber Attack Surface
Secure Design and Development

Cyber Attack Surface

- Supply chain attacks
  - Trusted boot
  - Hardware roots of trust
- OS vulnerabilities
  - Security updates / patches
  - Restrict SW installation
  - Upgrade aging / unsafe applications
  - OS hardening
- Network attacks
  - Close ports
  - Authenticate trusted devices
- Software vulnerabilities
  - Perform security tests
  - Coding standards (MISRA, SEI CERT C, …)
- Physical interfaces
  - Don’t expose unnecessary interfaces (JTAG, debug ports, …)
  - Sensors handle unexpected data
- Insider threats
  - Implement proper access control
  - Use secure network communications

Secure Design and Development

- Threat modeling
- Trust Boundaries
- Secure Design Principles
- Secure Coding Practices
- Secure instrument LAN communication and access

Secure Design
Threat Modeling

Threat-modeling methods are used to create

- An abstraction of the system
- Profiles of potential attackers, including their goals and methods
- A catalog of potential threats that may arise

Enables identifying the attack surfaces in your system design early in the design / development phases

- Threat Modeling: 12 Available Methods – Carnegie Mellon University

	Threat	Property Violated	Threat Definition
S	Spoofing identify	Authentication	Pretending to be something or someone other than yourself
T	Tampering with data	Integrity	Modifying something on disk, network, memory, or elsewhere
R	Repudiation	Non-repudiation	Claiming that you didn't do something or were not responsible; can be honest or false
I	Information disclosure	Confidentiality	Providing information to someone not authorized to access it
D	Denial of service	Availability	Exhausting resources needed to provide service
E	Elevation of privilege	Authorization	Allowing someone to do something they are not authorized to do

STRIDE evaluates the system detail design. It models the in-place system. By building data-flow diagrams (DFDs), STRIDE is used to identify system entities, events, and the boundaries of the system. STRIDE is implemented as part of the Microsoft Security Development Lifecycle (SDL) with the Threat Modeling Tool.

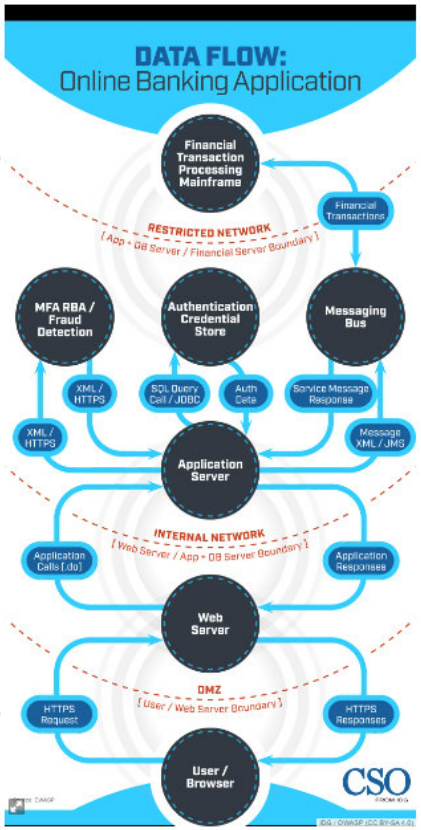
The Process for Attack Simulation and Threat Analysis (PASTA) is a risk-centric threat-modeling framework. PASTA aims to bring business objectives and technical requirements together. This method elevates the threat-modeling process to a strategic level by involving key decision makers and requiring security input from operations, governance, architecture, and development.

Secure Design
Trust Boundary

Trust Boundary

- Boundary where program data or execution changes its level of "trust" or where two principles with different capabilities exchange data or commands. (Wikipedia)
  - Execution trust boundary – application attains an increased privilege level
  - Data trust boundary – data comes from an untrusted source
- Trust boundaries can be identified as part of an overall threat modeling analysis of a system
- Trust boundaries indicate where to focus attention on securing a system design.

Trust Boundaries



Data flow diagram for an online banking application (from Wei Zhang & Marco Morana, distributed under the OWASP license)

Secure Design Principles & Secure Coding Practices

10 Secure Design Principles

Secure Your Environment:

1. Minimize attack surface area
2. Secure by default
3. Principle of defense in depth
4. Don't trust security through obscurity
5. Simplicity

Know and Limit Access:

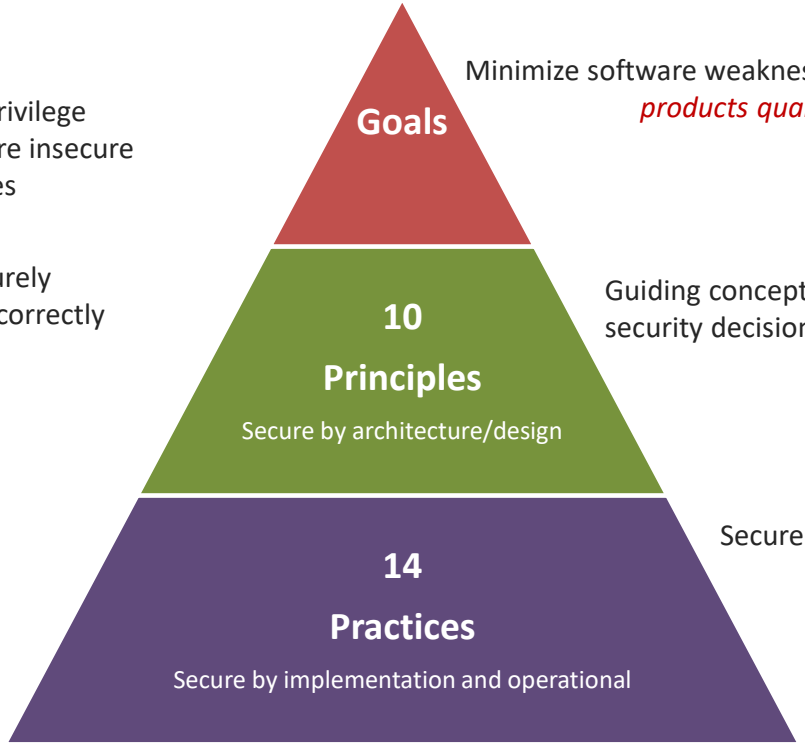
6. Principle of least privilege
7. External systems are insecure
8. Separation of duties

Detect and Respond:

9. Fail safely and securely
10. Fix security issues correctly

14 Secure coding practices

1. Input Validation
2. Output Encoding
3. Authentication and Password Management
4. Session Management
5. Access Control
6. Cryptographic Practices
7. Error Handling and Logging
8. Data Protection
9. Communication Security
10. System Configuration
11. Database Security
12. File Management
13. Memory Management
14. General Coding Practices



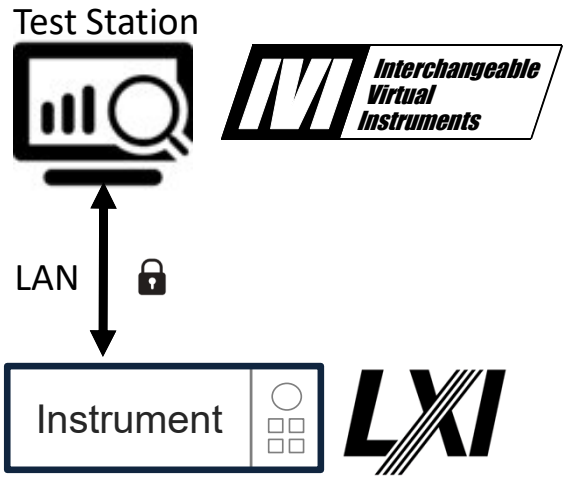
Minimize software weaknesses *(and improve products quality)*

Guiding concepts in making security decisions

Secure coding practices

Adapted from OWASP Guide v2.0.1

CYBERSECURITY ASSOCIATION OF MARYLAND, INC.

T&M Industry Security Standards

- Collaborative effort with IVI Foundation and LXI Consortium
  - Secure Instrument Communication
  - Secure LAN access to an instrument
- IVI Security Extensions
  - VISA (C/C++, COM, .NET) security extensions
  - HiSLIP r2.0 – authenticated / encrypted LAN communication
  - IVI SASL – align SASL authentication methods to use
- LXI Version 1.6
  - Security Extended Function – secure command-and-control and instrument's web interface
  - API Extended Function – REST API to query and configure the security and network settings of an instrument.
  - Device Specification – HTTPS instrument web server
  - Various other minor changes to address security and align with current network practices