



We're ready.
Are you?

Secure Design with Threat Modeling

Jim Spain – Technical Marketing Engineer

Agenda

- Secure Design Challenge
- Threat Modeling @ Cisco
(Process and Example)
- Results
- Q&A

Secure Design Challenge...

- Talented but Large Engineering Community (25K+)
- Diverse Product Line
- Security Focus is Critical
- Expanding Security Knowledge

Everyone Threat Models - Cars, Houses, Children?





“Structured and repeatable process to identify and mitigate threats”

- ✓ *Leads teams to consider potential attack vectors*
- ✓ *Exposes weaknesses other methods may not uncover*
- ✓ *Adds security focus without extensive security knowledge*
- ✓ *Finds vulnerabilities Early and Before First Customer Ship*

Approaches to Threat Modeling

Unstructured



Structured

Asset Centric

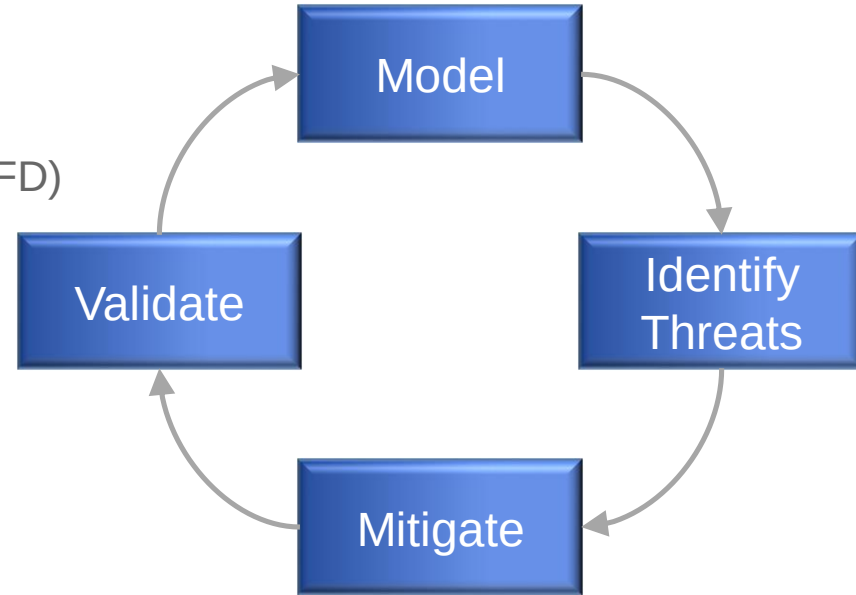
Attacker Centric

Software Centric

ThreatBuilder (Cisco Threat Modeling Tool)

Starts with the System Design

- **Cisco developed browser-based tool**
- **Activities**
 - Model the feature using a Data Flow Diagram (DFD)
 - Add attributes / Identify threats
 - Mitigate threats
 - Validate mitigations
- **Output**
 - Better view of the feature's threat landscape
 - Plan of action to close or reduce vulnerabilities



Threat Modeling @ Cisco

Definitions

- **Threat** - a real or theoretical scenario that may result in a product security issue
- **Element** – basic building block for a threat model Data Flow Diagram
- **Attribute** – label that gives definition to an element (functional, data)
- **Mitigation** – technical or procedural change to eliminate or lessen the ill effects of a threat
- **Validation** – a test or other proof of mitigation effectiveness

Cisco Threat Modeling Process

- **Modelers:**

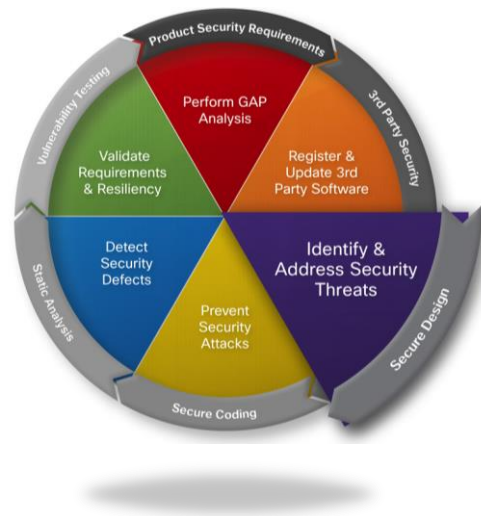
- *Engineers:* Dev Leads (Tech Leads, Architects, Principal Engineers)
- *Facilitators:* Security Advocates (SA), Security Engagement Mgr. (SEM)

- **Time Requirement:**

- 2 x engineers ~ 8 hours each for a basic model
- 3 x threat models per feature / component

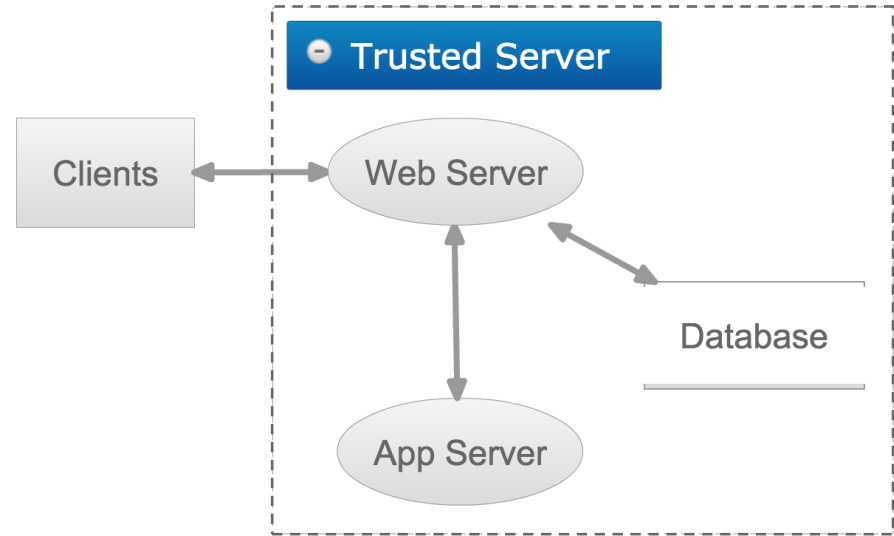
- **Workflow:**

- Before 1st Agile Commit
- Before Execution Commit (Waterfall)



Create the Data Flow Diagram (DFD)

- Graphically represent the feature under design
- Add elements, data flows, functions, protocols
- Establish elemental relationships



Add Attributes / Assign Threats

Attribute Details

Cryptographic

AttributeTree
Root>>Process>>Cryptographic

Description:
A process that is intended to provide confidentiality.

Associated Threats:

- Time and State Attacks (Process)
- Exploitation of Privilege/Trust (Process)
- Manipulate Resources (Process)
- Cryptanalysis (Cryptographic)
- Data Leakage Attacks (Process)
- Resource Depletion (Process)
- Injection (Injecting Control Plane content through the Data Plane) (Process)
- Deceptive Interactions (Process)
- Scanning for Vulnerable Software (Process)

Automated

CAPEC Common Attack Pattern Enumeration and Classification
A Community Resource for Identifying and Understanding Attacks

Home > CAPEC List > CAPEC-97: Cryptanalysis (Version 2.6)

CAPEC-97: Cryptanalysis
Attack Pattern ID: 97
Status: Draft
Completeness: Complete

Summary

Cryptanalysis is a process of finding weaknesses in cryptographic algorithms and using these weaknesses to decipher the ciphertext without knowing the secret key (instance deduction). Sometimes the weakness is not in the cryptographic algorithm itself, but rather in how it is applied that makes cryptanalysis successful. An attacker may have other goals as well, such as:

1. Total Break - Finding the secret key
2. Global Deduction - Finding a functionally equivalent algorithm for encryption and decryption that does not require knowledge of the secret key.
3. Information Deduction - Gaining some information about plaintexts or ciphertexts that was not previously known.
4. Distinguishing Algorithm - The attacker has the ability to distinguish the output of the encryption (ciphertext) from a random permutation of bits

The goal of the attacker performing cryptanalysis will depend on the specific needs of the attacker in a given attack context. In most cases, if cryptanalysis is successful at all, an attacker will not be able to go past being able to deduce some information about the plaintext (goal 3). However, that may be sufficient for an attacker, depending on the context.

Attack Prerequisites

- The target software utilizes some sort of cryptographic algorithm.
- An underlying weaknesses exists either in the cryptographic algorithm used or in the way that it was applied to a particular chunk of plaintext.
- The encryption algorithm is known to the attacker.
- An attacker has access to the ciphertext.

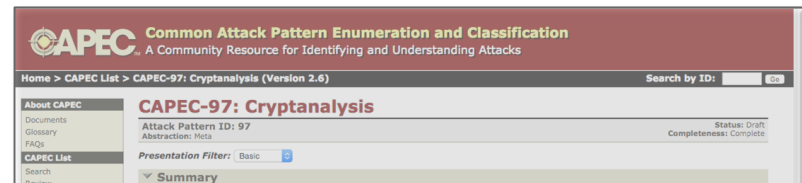
Solutions and Mitigations

Use proven cryptographic algorithms with recommended key sizes. Ensure that the algorithms are used properly. That means:

1. Not rolling out your own crypto; Use proven algorithms and implementations.
2. Choosing initialization vectors with sufficiently random numbers
3. Generating key material using good sources of randomness and avoiding known weak keys
4. Using proven protocols and their implementations.
5. Picking the most appropriate cryptographic algorithm for your usage context and data

Mitigate Threats

- Apply Default Mitigations (CAPEC, Cisco Specific, etc.)
- Apply Cisco proprietary solutions
- Redesign to reduce or remove the threat

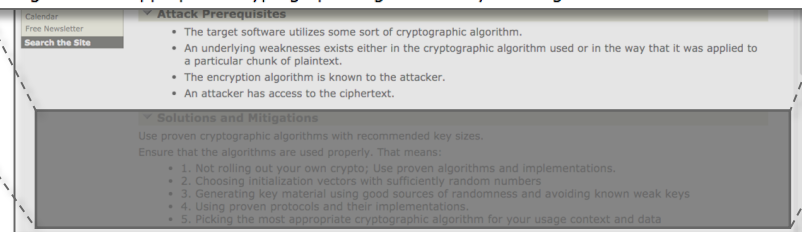


▼ Solutions and Mitigations

Use proven cryptographic algorithms with recommended key sizes.

Ensure that the algorithms are used properly. That means:

- 1. Not rolling out your own crypto; Use proven algorithms and implementations.
- 2. Choosing initialization vectors with sufficiently random numbers
- 3. Generating key material using good sources of randomness and avoiding known weak keys
- 4. Using proven protocols and their implementations.
- 5. Picking the most appropriate cryptographic algorithm for your usage context and data



Validate Mitigations

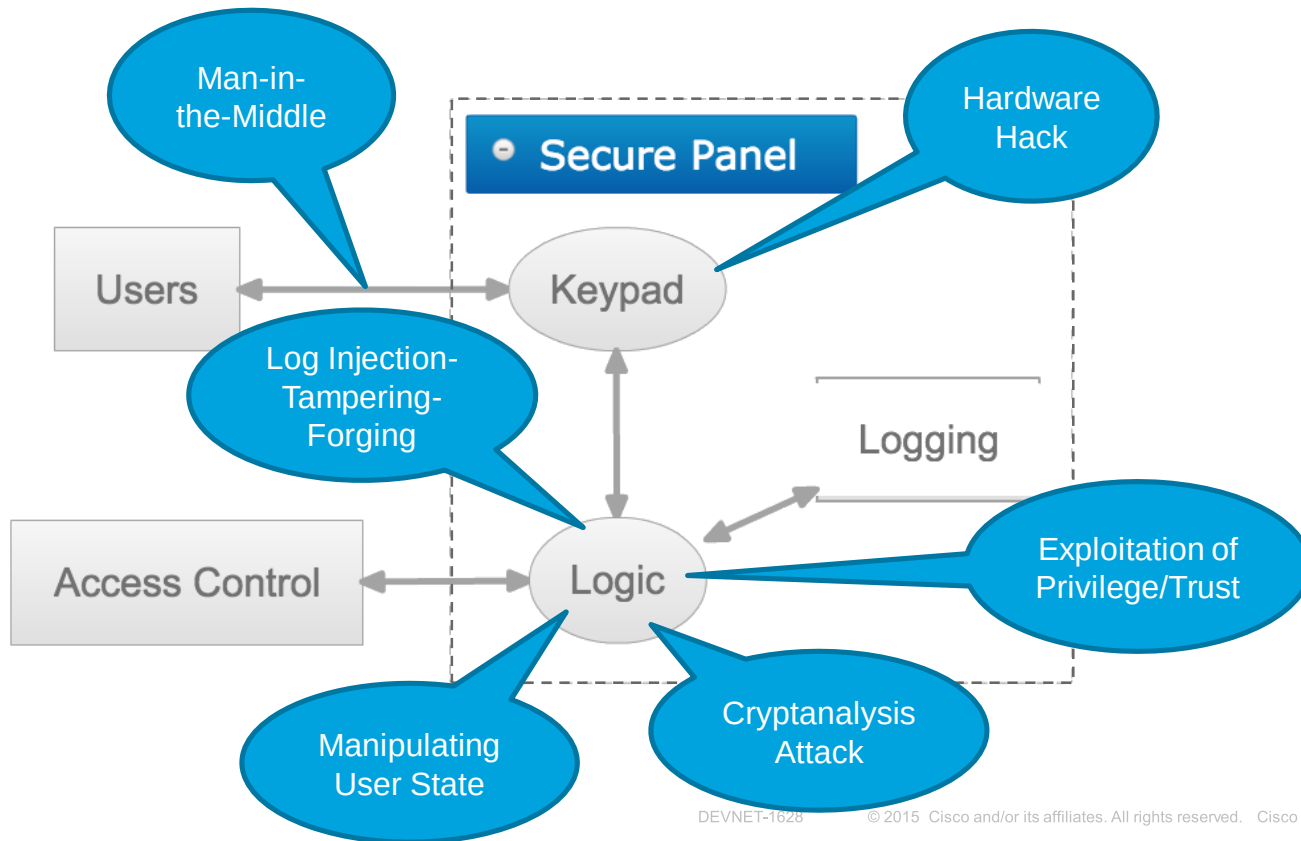
- Validations “prove” mitigations
 - Create and execute test cases
 - File bugs with the proper tracking attributes
- Review & explore the solution
 - Is the model correct for future product iterations?
 - Consider changes in design and implementation
 - Consider anomalies found during the test cycle



Elevator Control Panel (Secure)



Threat Modeling Data Flow Diagram



Results

Example Results – Bug Created and Filed

The screenshot displays the Threat Builder application window. On the left, the 'Threat List' pane shows a tree view of threat categories. The 'Exploitation of Privilege/Trust' category is selected, and its sub-entry 'Exploitation of Privilege/Trust diagram Element : YYZ (server)' is highlighted in blue. To the right of this entry, the word 'High' is displayed in red. The main 'Threat Detail' pane on the right shows the details for the selected threat. The 'Threat' field contains 'Exploitation of Privilege/Trust'. The 'Diagram Element' is 'Exploitation of Privilege/Trust Group'. The 'Description' field contains a detailed paragraph about the attack mechanism. The 'Analysis' section contains three lines of text. The 'Mitigations' section contains two items, with the first item 'Implement authentication' marked as 'Mandatory'. The 'Validation Techniques' section is empty. The 'Priority' tab is selected, showing 'Potential Impact' as 'High', 'Applicability' as 'Valid Threat', and 'Completeness' as 'Not Mitigated'. A red circle is drawn around the 'Analysis' and 'Mitigations' sections.

Threat List Total Threats : 46

Group By: Threat Name Sort By: Potential Impact

- API Abuse/Misuse
- Authentication Bypass
- Buffer Overflow in an API Call
- Client-Server Protocol Manipulation
- Cryptanalysis
- Data Leakage Attacks
- Deceptive Interactions
- Exploitation of Privilege/Trust** High
- Exploitation of Session Variables, Resource IDs and other Trusted Credentials
- Exploiting Low Grade Encryption
- Exploiting Multiple Input Interpretation Layers
- Fuzzing
- HTTP Parameter Pollution (HPP)
- Harvesting Usernames or UserIDs via Application API Event Monitoring
- Injection (Injecting Control Plane content through the Data Plane)

Threat Detail

Threat: Exploitation of Privilege/Trust Reset Threats

Diagram Element: Exploitation of Privilege/Trust Group

Description: (Details...)

An attacker actively targets exploitation of weaknesses, limitations and assumptions in the mechanisms a target utilizes to manage access to its resources or authorize utilization of its functionality. Such exploitation can lead to the complete subversion of any control the target has over its data or functionality enabling almost any desired action on the part of the attacker. Weaknesses targeted by these sorts of attacks are often due to three primary factors: 1) a fundamental dependence on authentication mechanisms being effective; 2) a lack of effective control over the separation of privilege between various entities; and 3) assumptions and overconfidence in the strength or rigor of the implemented authorization mechanisms.

Analysis:

The YYZ server needs to implement an authentication check.

This task has been identified and under development.

CSCuvBR549 has been created to track this work.

Mitigations:

- Implement authentication** Mandatory
- The YYZ checks the request and reject any without the
- Authorization header or contain credentials that are not known to the system. The credential check is done via an API call to the AAA ...

Validation Techniques:

Priority Attributes

Potential Impact: High

Applicability: Valid Threat

Completeness: Not Mitigated

☐ Validated

Example Results – Protocol Requirement

The screenshot displays the 'Threat Builder' application window. The left pane, titled 'Threat List', shows a list of threats, all labeled 'Man in the Middle Attack' with a 'Very High' severity. The right pane, titled 'Threat Detail', provides information for the selected threat.

Threat List:

- Group By: Element
- Sort By: Potential Severity
- Total Threats: 294

Threat Detail:

- Threat:** Man in the Middle Attack
- Diagram Element:** XMPP/TLS Client to/from XMPP Server
- Description:** (Details...)
- Analysis:** This is a valid threat for XMPP because sensitive information is exchanged between XMPP client and XMPP server in cleartext format. XMPP is only recommended in controlled/secured network. XMPP TLS is always more secure to use.
- Mitigations:** XMPP TLS (Recommended) - Use XMPP TLS over XMPP. XYZ supports communication over XMPP TLS.
- Validation Techniques:**

Attributes:

- Potential Impact:** Very High
- Applicability:** Valid Threat
- Completeness:** Not Mitigated
- ☐ Validated

Example Results – Documentation

The screenshot displays the 'Threat Builder' application interface. On the left, the 'Threat List' pane shows a table of threats, all categorized as 'Data Leakage Attacks' or 'Resource Depletion' with a 'High' severity. The 'Threat Detail' pane on the right provides a comprehensive view of a selected 'Resource Depletion' threat. This pane includes a 'Threat' name, a 'Diagram Element' (Syslog to/from Syslog Server), a 'Description', an 'Analysis' section, 'Mitigations', and 'Validation Techniques'. A red oval is drawn around the 'Mitigations' and 'Validation Techniques' sections, indicating the focus of the documentation example.

Threat List Total Threats : 294

Group By: Element Sort By: Potential Severity

Threat Detail

Threat: Resource Depletion Reset Threat

Diagram Element: Syslog to/from Syslog Server

Description: (Details...)

An attacker depletes a resource to the point that the target's functionality is affected. Virtually any resource necessary for the target's operation can be targeted in this attack. The result of a successful resource depletion attack is usually the degrading or denial of one or more services offered by the target. Resources required will depend on the nature of the resource to be depleted, the amount of the resource the target has access to, and other mitigating circumstances such as the target's ability to shift load, detect and mitigate resource depletion attacks, or acquire additional resources to deal with the depletion.

Priority: Attributes

Potential Impact: High

Applicability: Valid Threat

Completeness: Mitigated ☐ Validated

Analysis:

Extremely high volumes of logs can be generated by Syslog, specially if Verbose settings is turned on. This can also consume a major amount of network bandwidth, which might slow down XYZ Server performance.

Mitigations:

Documentation Better than Nothing

User docs mention the possibility of high volume of syslogs. It's upto customer's discretion to maintain the level of logging.

Validation Techniques:

Summary

- Secure networks require secure products
- Threat modeling changes our approach to security
- Add threat modeling to your project
- Cisco wants to be your most trusted IT partner

Q & A

Complete Your Online Session Evaluation

Give us your feedback and receive a **Cisco 2016 T-Shirt** by completing the Overall Event Survey and 5 Session Evaluations.

- Directly from your mobile device on the Cisco Live Mobile App
- By visiting the Cisco Live Mobile Site
<http://showcase.genie-connect.com/ciscolivemelbourne2016/>
- Visit any Cisco Live Internet Station located throughout the venue

T-Shirts can be collected Friday 11 March at Registration

Cisco *live!*
DevNet Program



Learn online with Cisco Live!
Visit us online after the conference for full access to session videos and presentations.

www.CiscoLiveAPAC.com



Thank you

