Using Threat Models for incidents;
Introducing the possible and impossible attack trees.

@TashJNorris
Head of Product Security @ Moonpig
The topic presented here is intended to be complementary to existing incident response processes and not a complete replacement.
About Me

- Head of Product Security @ Moonpig
- OWASP WIA London co-founder
- @TashJNorris - Twitter | Medium
01

Threat Modelling
Threat Modelling
The Four Questions

1. What am I building?
2. What can go wrong?
3. Did I do a good job in steps 1-3?
4. What can I do about it?

Credit: Adam Shostack
SDLC Process

Secure Software Development Lifecycle

DESIGN
- Threat models
- Secure architecture

CONSTRUCTION
- Review board
- Secure coding standards and practices
- Cppcheck, Coverity
- Training
- Boot camps
- Brown bags

VULNERABILITY RESPONSE
- Ratings
- Response process
- Quick response
- Complete fix
- Solution publishing
- Regression testing

TEST
- Internal security tests
- Fuzzers, scanners, BVTS
- Third-party penetration testing

Credit: F5 Platform Security Whitepaper
SDLC Process

Credit: Hemanth Srinivasan
SDLC Process

Credit: Tash Norris
Threat Modelling

- Threat Modelling is traditionally suggested for use at the ‘Design Phase’, when actually it CAN be used at any point.

   ‘The earlier the better, but never too late’

- There are many ways to threat model pick whichever works for you.
02

Kill chain
# Kill Chain

<table>
<thead>
<tr>
<th>Phase</th>
<th>Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reconnaissance</td>
<td>• Harvesting email addresses, conference information, etc.</td>
</tr>
<tr>
<td>Weaponization</td>
<td>• Coupling exploit with backdoor into deliverable payload</td>
</tr>
<tr>
<td>Delivery</td>
<td>• Delivering weaponized bundle to the victim via email, web, USB, etc.</td>
</tr>
<tr>
<td>Exploitation</td>
<td>• Exploiting a vulnerability to execute code on victim’s system</td>
</tr>
<tr>
<td>Installation</td>
<td>• Installing malware on the asset</td>
</tr>
<tr>
<td>Command &amp; Control (C2)</td>
<td>• Command channel for remote manipulation of victim</td>
</tr>
<tr>
<td>Actions on Objectives</td>
<td>• With “Hands on Keyboard” access, intruders accomplish their original goal</td>
</tr>
</tbody>
</table>
03

Attack Trees
Introducing Attack Trees
Introducing Attack Trees..

Credit: Bruce Schneier
Attack Trees..
04
An incident lifecycle with attack trees
ATTACKS EXPERIENCED

VIRUSES
27%
*incl. ransomware

SPYWARE

MALWARE

IMPERSONATION
28%
EMAILS

PHISHING
80%

Pick an incident

Credit: UK Gov 2019 Cyber Survey | Atlas Cloud infographics
The extended incident team

SOC Analyst

AppSec/Cloud Sec Team

Engineering Team
Understand the what.
Incident Attack Trees

- The Incident
- Cause
  - Vector 1
  - Vector 2
  - Vector 3
  - Vector 4
Incident Attack Trees
Incident Attack Trees

- **Cause**
  - Vector 1
  - Vector 2
  - Vector 3
  - Vector 4

- **Symptom**
  - Vulnerability (Vuln)
  - Non-Security Knowledge (NSK)

- **The Incident**
  - Protection (P)
  - Information (I)

---

The diagram illustrates the relationship between causes and symptoms, with lines indicating the flow of information or protection status.
Incident Attack Trees
Incident Attack Trees

Diagram showing the sequence of events and attack vectors in an incident.
The extended incident team

- SOC Analyst
- AppSec/Cloud Sec Team
- Engineering Team
04

The impossible part..
The extended POST-incident team

SOC Analyst

AppSec/Cloud Sec Team

Engineering Team
The impossible paths
Feature: User Data contains sensitive information

In order to obtain sensitive information about the target
As an attacker
I want the target to have inappropriately placed sensitive information in User Data that I can access

Scenario Outline: Access via instance attribute

Given an instance with sensitive information in the User Data attribute
And a principal with the ability to read the instance attributes
When the attacker searches the User Data for the "<data-type>"
Then the sensitive information is returned to the attacker

Examples: Data types

<table>
<thead>
<tr>
<th>data-type</th>
</tr>
</thead>
<tbody>
<tr>
<td>password</td>
</tr>
<tr>
<td>API key</td>
</tr>
<tr>
<td>X.509 private key</td>
</tr>
<tr>
<td>SSH private key</td>
</tr>
<tr>
<td>Internal URL</td>
</tr>
</tbody>
</table>
Revisit controls

- **91%**: apply patches as soon as available
- **70%**: only allow access via company devices
- **65%**: backup (62% backup using a cloud service)
- **40%**: monitor user activities

Credit: UK Gov 2019 Cyber Survey | Atlas Cloud infographics
Update the playbook

If you attack tree discovered other attack vectors we can ensure the playbook covers those too
Attack Trees

- Used by the wider team to guide RCA's
- Complementary to existing processes
- Can be used to create and update playbooks
- Use to predict potential incidents

They're a bit of an art form; subjective, occasionally ugly and confusing but they can be valuable.
Did I do a good job?

Write tests
Validate the impossible is [still] impossible over and over..

Revisit Controls
Are the controls sufficient, is there anything else that can be done, should we revisit accepts?

Update Playbooks
Iterate. Take what we’ve learnt and iterate.
CREDITS

- Threat Modelling: Designing for Security - Adam Shostack
- Attack Trees; Modelling security threats - B. Schneier
- OWASP Cloud Security project
- Gov UK 2019 threat survey report