Incremental Threat Modelling

Irene Michlin
Principal Security Consultant
Never try to boil an ocean
Who am I

• Coming from software development and architecture
  • 20 years as software engineer, architect, technical lead

• Variety of consulting and testing work
  • From corporations to start-ups

• Favourite engagement type – threat modelling
• STRIDE – quick recap
• Introducing our example
• Incremental modelling walk-through
• Sting in the tail
• Conclusions
• Q&A
Threat modelling - reminder

• Decompose architecture using DFDs
• Search for threats using STRIDE
• Rank or quantify – out of scope for today
# Data Flow Diagrams

<table>
<thead>
<tr>
<th>External Entity</th>
<th>Process</th>
<th>Data Flow</th>
<th>Data Store</th>
<th>Trust Boundary</th>
</tr>
</thead>
<tbody>
<tr>
<td>People</td>
<td>Logical component</td>
<td>RPC</td>
<td>Database</td>
<td>Process boundary</td>
</tr>
<tr>
<td>Other systems</td>
<td>Service</td>
<td>Network traffic</td>
<td>File</td>
<td>Network boundary</td>
</tr>
<tr>
<td></td>
<td>Process in memory</td>
<td>File I/O</td>
<td>Queue/Stack</td>
<td></td>
</tr>
</tbody>
</table>

- People
- Other systems
- Logical component
- Service
- Process in memory
- RPC
- Network traffic
- File I/O
- Database
- File
- Queue/Stack
- Process boundary
- Network boundary
<table>
<thead>
<tr>
<th>Threat</th>
<th>Property</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoofing</td>
<td>Authentication</td>
<td>Impersonating something or someone else</td>
</tr>
<tr>
<td>Tampering</td>
<td>Integrity</td>
<td>Modifying data or code</td>
</tr>
<tr>
<td>Repudiation</td>
<td>Non-repudiation</td>
<td>Claiming to have not performed an action</td>
</tr>
<tr>
<td>Information Disclosure</td>
<td>Confidentiality</td>
<td>Exposing information to non-authorised party</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>Availability</td>
<td>Deny or degrade service</td>
</tr>
<tr>
<td>Elevation of Privilege</td>
<td>Authorization</td>
<td>Gain capabilities without proper authorisation</td>
</tr>
</tbody>
</table>
Introducing our example

• Explain the existing architecture and the feature we are planning to add
• Pretend that threat model for the existing part does not exist
• Model new feature
A very simple architecture
We are going to use a 3rd party reporting and analytics technology. They are going to host Data Warehouse (DWH) and reporting server on their infrastructure. They will give us licences to use their web-based Analytics App, which can query the reporting server. The only thing we need to build in-house is an aggregator process, which will get data from our database, aggregate it and upload it to the DWH on a regular basis (they provide API for automated upload).
Step by step

We are going to use a 3rd party reporting and analytics technology. They are going to host Data Warehouse (DWH) and reporting server on their infrastructure.

They will give us licences to use their web-based Analytics App, which can query the reporting server. The only thing we need to build in-house is an aggregator process, which will get data from our database, aggregate it and upload it to the DWH on a regular basis (they provide API for automated upload).
Step by step

We are going to use a 3rd party reporting and analytics technology. They are going to host Data Warehouse (DWH) and reporting server on their infrastructure. They will give us licences to use their web-based Analytics App, which can query the reporting server. The only thing we need to build in-house is an aggregator process, which will get data from our database, aggregate it and upload it to the DWH on a regular basis (they provide API for automated upload).
Step by step

We are going to use a 3rd party reporting and analytics technology. They are going to host Data Warehouse (DWH) and reporting server on their infrastructure. They will give us licences to use their web-based Analytics App, which can query the reporting server. The only thing we need to build in-house is an aggregator process, which will get data from our database, aggregate it and upload it to the DWH on a regular basis (they provide API for automated upload).
Step by step

We are going to use a 3rd party reporting and analytics technology. They are going to host Data Warehouse (DWH) and reporting server on their infrastructure.

They will give us licences to use their web-based Analytics App, which can query the reporting server. The only thing we need to build in-house is an aggregator process, which will get data from our database, aggregate it and upload it to the DWH on a regular basis (they provide API for automated upload).
Step by step

We are going to use a 3rd party reporting and analytics technology. They are going to host Data Warehouse (DWH) and reporting server on their infrastructure. They will give us licences to use their web-based Analytics App, which can query the reporting server. The only thing we need to build in-house is an aggregator process, which will get data from our database, aggregate it and upload it to the DWH on a regular basis (they provide API for automated upload).
Last step

We are going to use a 3rd party reporting and analytics technology. They are going to host Data Warehouse (DWH) and reporting server on their infrastructure.

They will give us licences to use their web-based Analytics App, which can query the reporting server. The only thing we need to build in-house is an aggregator process, which will get data from our database, aggregate it and upload it to the DWH on a regular basis (they provide API for automated upload).
Last step
Relevant Threats

**Spoofing**
- Can attacker upload data on our behalf? How we authenticate the destination before uploading?

**Tampering and Information Disclosure**
- Can attacker sniff the data or tamper with it?

**Repudiation**
- Can DWH claim we didn’t send the data? Or sent above the quota?

**Denial of service**
- Is there availability SLA for uploads?

**Privacy**
- Can our aggregation be reverse engineered?
- Do we need to notify the users that 3rd party is involved?
Irrelevant Threats
How to make them go away

• Can registered user inject malicious content?
  • We are not making it worse
• Can anonymous user bypass access controls and modify something?
  • We are not making it worse
• Is our datacentre infrastructure secure?
  • We are not making it worse (careful here!)
• Can analytics user abuse licencing?
  • Not our problem, 3\textsuperscript{rd} party problem
Caveats

Not our problem

• If the team’s task is not just to implement with a chosen provider, but to evaluate several providers.

We are not making it worse

• If you come across something so catastrophic in the “Legacy blob”, that it’s an immediately obvious critical flaw.
What if implementation deviates from design?

• Aggregator is implemented as two processes: one to read and aggregate the data, the other for actual upload.

• Time pressure and we MUST have analytics in the release. Let’s create a user for this 3rd party so they pull data directly from our DB.
Looks familiar?

1. Untested (ball of mud) legacy code
2. Introducing tests for new and modified code
3. Eventually getting (almost) fully tested code
This does not work in security!

• NTVDM bug – found in 2010, introduced in 1993
• Shellshock – found in 2014, introduced in 1989
• Heartbleed – found in 2014, introduced in 2011
• POODLE – found in 2014, existed since 1996
• JASBUG – found in 2015, introduced in 2000
• DROWN, Badlock, gotofail, etc.
Eventually need the whole picture

• What we don’t know can harm us
• The system is greater than the sum of its parts
Eventually is better than upfront

- People have developed the necessary skills
- Many subsystems will be already analysed
- Easier to achieve management buy-in
Conclusion

• Incremental threat modelling can fit any time-box, without disturbing the regular development cadence.

• You can build a model of the whole system in parallel, starting from day 1, or waiting for several cycles, whatever suits your situation.

• As a shortcut, you can bring external resources to help with the initial model.

• But for the best results in agile environment you have to involve the whole team.
Conclusion
Points of contact

Irene Michlin
Principal Security Consultant

M: +44 (0) 7972 333 148
E: irene.michlin@nccgroup.trust
T: @IreneMichlin
Thank You to Our Sponsors

CME Group

SYNOPSYS

Hewlett Packard
Enterprise

ARXAN

BLACKDUCK

CHECKMARX

CITRIX®

FLEXERA
SOFTWARE

kiuwan

netsparker®

POSITIVE TECHNOLOGIES

RAPID7

Sonatype

Twistlock®

Invest
Northern
Ireland

TechChannels

jscrambler

Invest
Northern
Ireland

MCS GROUP

edgescan

Invest
Northern
Ireland

Allstate

WhiteHat
SECURITY