Security Risk Metrics

Prof. Dr. Raimundas Matulevičius

University of Tartu, Estonia, rma@ut.ee
Security Risk Management
Domain Model
Asset-related Concepts

• **Business asset**
  – Caveman’s ability to observe the surrounding world (to search for food)

• **IS asset**
  – Caveman
  – A cave (from which the caveman monitors the world)

• **Security criterion**
  – Availability of the caveman’s ability to observe the surrounding world
  – *Integrity of the* caveman’s ability to observe the surrounding world
Security Risk Management
Domain Model

- **Security needs**
  - Security objective that characterizes the application of a *security criterion* on a *business asset*

- **Business asset Value**
  - Only business assets are estimated in terms of value
  - Business assets are involved to define and estimate security objectives and to assess the significance of risk
Measuring Assets

<table>
<thead>
<tr>
<th>Caveman’s ability to observe the surrounding world (to search for food)</th>
<th>Value</th>
<th>= 30</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security need for availability</td>
<td>= 3</td>
<td></td>
</tr>
<tr>
<td>Security need for integrity</td>
<td>= 1</td>
<td></td>
</tr>
<tr>
<td>Security need for confidentiality</td>
<td>= 0</td>
<td></td>
</tr>
</tbody>
</table>
Risk-related Concepts

- **Risk**
  - Dino assaults through the cave hole because he is able to get through it, and eats the caveman thus leading to the extinct of cavemen

- **Impact**
  - Harms caveman;
  - The cave is not reliable;
  - Negates availability of the caveman
  - Leads to the extinct of cavemen (because nobody would feed the rest of the family)

- **Event**
  - Dino assaults through the cave hole because he is able to get through it, and eats the caveman

- **Vulnerability**
  - The cave hole is large enough for the Dino to get in

- **Threat**
  - Dino assaults through the cave hole and eats the caveman

- **Threat agent**
  - Dino, who has teeth, and is hungry

- **Attack method**
  - Assault through the cave hole;
  - Eat the caveman
Security Risk Management

Domain Model

- **Risk level**
  - Depends on event potentiality and impact level

- **Potentiality**
  - Is estimated through threat likelihood and vulnerability level
# Measuring Risk

## Threat likelihood that Dino assaults through the cave hole and eats the caveman

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Unlikely, regarding the statistics or the necessary Dino’s competence (our Dinos are vegetarians! Dino’s teeth are not strong enough)</td>
</tr>
<tr>
<td>2</td>
<td>Can happen, but there is only one Dino in the area, most probably he will not find the cave</td>
</tr>
<tr>
<td>3</td>
<td>Can happen, there are a lot of Dinos around and their favourite dish is cavemen (“my neighbour was eaten yesterday!!!”)</td>
</tr>
</tbody>
</table>

## Level of vulnerability: The cave hole is large enough for the Dino to get in

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Very low – security measures in place and so far no Dinos got into the cave</td>
</tr>
</tbody>
</table>
| 1     | Medium – no effective security measures in place  
(there is a bludgeon but no effective bone-teeth on it) |
| 2     | Very high – lack of security measure, obsolete or not applied |
Measuring Risk

- Potentiality of Event = likelihood + vulnerability level – 1
  - 3+2-1 = 4

- Maximum impact level of concerned impacts for the studied business assets; estimated from the security needs

<table>
<thead>
<tr>
<th>Impact level</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potentiality</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
</tr>
</tbody>
</table>
Risk Treatment-related Concepts

Risk treatment decision
- Risk reduction (reduce number of Dinos)

Security requirement
- Smash Dino hard – *bone-teeth*

Control
- A bludgeon with bone-teeth

Risk treatment decision
- Risk avoidance

Security requirement
- Prevent access to caveman

Control
- Metal bars on the cave hole
• **Cost**
  - Cost of buying a firewall
  - Cost of maintaining it by a security officer

• **Risk reduction**
  - Risk *reduction, avoidance and transfer* treatment
  - For risk *retention* risk reduction equals 0
# Measuring Risk Treatment

<table>
<thead>
<tr>
<th>Risk treatment</th>
<th>Risk reduction</th>
<th>Risk avoidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security requirement</td>
<td>New vulnerability level</td>
<td>Smash Dino hard</td>
</tr>
<tr>
<td>New Risk level</td>
<td>9</td>
<td>6</td>
</tr>
<tr>
<td>Risk reduction</td>
<td>3</td>
<td>6</td>
</tr>
</tbody>
</table>
# Measuring Risk Treatment

<table>
<thead>
<tr>
<th>Risk treatment</th>
<th>Risk reduction</th>
<th>Risk avoidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security requirement</td>
<td>Smash Dino hard</td>
<td>Prevent access to caveman</td>
</tr>
<tr>
<td>New vulnerability level</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>New Risk level</td>
<td>9</td>
<td>6</td>
</tr>
<tr>
<td>Risk reduction</td>
<td>3</td>
<td>6</td>
</tr>
</tbody>
</table>

**Cost of**
- A bludgeon with bone-teeth = 5
- Metal bars on the cave hole = 15
# Measuring Risk Treatment

<table>
<thead>
<tr>
<th>Security requirement</th>
<th>New vulnerability level</th>
<th>Risk reduction</th>
<th>Risk avoidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smash Dino hard</td>
<td>1</td>
<td>Prevent access to caveman</td>
<td>0</td>
</tr>
</tbody>
</table>

- Cost of:  
  - A blunt object  
  - Metal bars on the cave hole = 15
**Return on Security Investment**

\[
ROSI = \left( \frac{RiskExposure \times RiskMitigated}{SolutionCost} \right) \times 100\%
\]

- **A bludgeon with bone-teeth**
  - Risk exposure = 30
  - Risk mitigated = Risk reduction / Risk level = 3/12
  - Solution cost = 5
  
  \[
  ROSI \text{ (A bludgeon with bone-teeth)} = 50\%
  \]

- **Metal bars on the cave hole**
  - Risk exposure = 30
  - Risk mitigated = Risk reduction / Risk level = 6/12
  - Solution cost = 15
  
  \[
  ROSI \text{ (Metal bars on the cave hole)} = 0\%
  \]
A case of

Airline Turnaround

(Matulevičius, Norta et al, 2016)

- Catering
- Ramp service
  - Luggage handling
  - Refueling
  - Air cargo handling
- Passenger service
  - Check-in
  - Gate arrival
- Field operation service
Flying On Airline Ticket In Someone Else’s Name?

MAY 3, 2014 BY LUCKY

I Got Through Airport Security With Someone Else’s Plane Ticket

NOVEMBER 19, 2015 / by THEHIPMUNK

What To Do if Something Gets Stolen from Your Luggage at the Airport

A TSA agent revealed the first steps travelers can take if property is lost or stolen.

Family: In-flight meal killed flier

By A. Pawlowski, CNN

Dozens of passengers told CNN they were served food they say made them sick.

New Tactics in the Fight Against Stolen Luggage

Stop Baggage Theft, TSA and Airports Use High-Definition Cameras, Fancy Pens

Sixty children taken sick during flight

This story was published: 3 YEARS AGO | MAY 08, 2014 8:56AM
Over the weekend I attended sessions. We took questions to get through all of them, so I fig...
US Airways Express Flight 5481 stalled after take-off (January 8, 2003), crashed into a US Airways hangar and burst into flames 37 seconds after leaving Charlotte/Douglas International Airport.

Although the pilots had totaled up the take-off weight of the aircraft before the flight and determined it to be within limits, the plane was actually overloaded and out of balance …
Security Risk Management in
Airline Turnaround Sector

- **Check-in passenger information**
  - *Risk1*: Blacklisted passenger presents fake document, gets checked-in because personnel could be bribed
  - *Risk2*: Attacker uses phishing email to extract passenger booking number and uses it to check-in to the flight

- **Luggage information**
  - *Risk3*: The personnel records values lower than actual weight of luggage and ground operations uses the information in the loading of the aircraft
  - *Risk4*: The personnel accepts luggage and adds contraband items to a passenger’s luggage

- **Fuel slip**
  - *Risk5*: A malicious insider with access to the computer that stores the fuel slip performs changes to the data contained in the fuel slip
  - *Risk6*: The attacker intercepts the fuel slip, changes the data contained and sends it to the supplier

- **Cargo assignment**
  - *Risk7*: A malicious insider with access rights performs changes to the cargo assignment document before it is sent to a service provider
  - *Risk8*: An attacker hacks the airline mailing list, receives the cargo assignment, changes the data contained and sends the cargo assignment to a service provider
Security Risk Management in 
Airline Turnaround Sector

- Check-in passenger information
  - Risk1: Blacklisted passenger presents fake document, gets checked-in because personnel could be bribed
  - Risk2: Attacker uses phishing email to extract passenger booking number and uses it to check-in to the flight

- Luggage information
  - Risk3: The personnel records values lower than actual weight of luggage and ground operations uses the information in the loading of the aircraft
  - Risk4: The personnel accepts luggage and adds contraband items to a passenger’s luggage

- Fuel slip
  - Risk5: A malicious insider with access
  - Risk6: The attacker intercepts the fuel slip, changes the data contained and sends it to the supplier

- Cargo assignment
  - Risk7: A malicious insider with access
  - Risk8: An attacker hacks the airline mailing list, receives the cargo assignment, changes the data contained and sends the cargo assignment to a service provider
Security Risk Management in Airline Turnaround Sector

- **Check-in passenger information**
  - **Risk1**: Blacklisted passenger presents fake document, gets checked-in because personnel could be bribed.

- **Fuel slip**
  - **Risk5**: A malicious insider with access to the computer that stores the fuel slip performs changes to the data contained in the fuel slip.

- **Luggage information**
  - **Risk3**: The personnel records values lower than actual weight of luggage and ground operations uses the information in the loading of the aircraft.
  - **Risk4**: The personnel accepts luggage and adds contraband items to a passenger’s luggage.

- **Cargo assignment**
  - **Risk7**: An attacker hacks the airline mailing list, receives the cargo assignment, changes the data contained and sends the cargo assignment to a service provider.

---

<table>
<thead>
<tr>
<th>Risk</th>
<th>Before treatment</th>
<th>After treatment</th>
<th>Risk reduction level</th>
<th>Business asset value</th>
<th>Cost of counter-measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk1</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>3</td>
<td>12</td>
</tr>
<tr>
<td>Risk2</td>
<td>2</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>15</td>
</tr>
<tr>
<td>Risk3</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Risk4</td>
<td>4</td>
<td>2</td>
<td>5</td>
<td>3</td>
<td>15</td>
</tr>
<tr>
<td>Risk5</td>
<td>3</td>
<td>3</td>
<td>5</td>
<td>4</td>
<td>20</td>
</tr>
<tr>
<td>Risk6</td>
<td>3</td>
<td>2</td>
<td>4</td>
<td>4</td>
<td>16</td>
</tr>
<tr>
<td>Risk7</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>3</td>
<td>12</td>
</tr>
<tr>
<td>Risk8</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>3</td>
<td>9</td>
</tr>
</tbody>
</table>
Security Risk Management in Airline Turnaround Sector

- **Risk1**: Blacklisted passenger presents fake document, gets checked-in because personnel could be bribed.

- **Risk2**: Attacker uses phishing email to extract passenger booking number and uses it to check-in to the flight.

- **Risk3**: The personnel records values lower than actual weight of luggage and ground operations uses the information in the loading of the aircraft.

- **Risk4**: The personnel accepts luggage and adds contraband items to a passenger’s luggage.

- **Fuel slip**
  - **Risk5**: A malicious insider with access to the computer that stores the fuel slip performs changes to the data contained in the fuel slip.
  - **Risk6**: The attacker intercepts the fuel slip, changes the data contained, and sends it to the supplier.

- **Luggage information**
  - **Risk7**: A malicious insider with access rights performs changes to the cargo assignment document before it is sent to a service provider.
  - **Risk8**: An attacker hacks the airline mailing list, receives the cargo assignment, changes the data contained, and sends the cargo assignment to a service provider.
## Security Risk Management in Airline Turnaround Sector

### Check-in passenger information
- **Risk 1**: Blacklisted passenger presents fake document, gets checked-in because personnel could be bribed.

### Luggage information
- **Risk 3**: The personnel records values lower than actual weight of luggage and ground operations uses the information in the loading of the aircraft.
- **Risk 4**: The personnel accepts luggage and adds contraband items to a passenger’s luggage.

<table>
<thead>
<tr>
<th>Risk</th>
<th>Value-RRL</th>
<th>RRL-cost</th>
<th>Value-cost</th>
<th>Graph 1</th>
<th>Graph 2</th>
<th>Graph 3</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk 1</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>5</td>
<td></td>
<td></td>
<td>Medium priority</td>
</tr>
<tr>
<td>Risk 2</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>7</td>
<td></td>
<td></td>
<td>High priority</td>
</tr>
<tr>
<td>Risk 3</td>
<td>1</td>
<td>2</td>
<td>2</td>
<td>5</td>
<td></td>
<td></td>
<td>Medium priority</td>
</tr>
<tr>
<td>Risk 4</td>
<td>2</td>
<td>3</td>
<td>2</td>
<td>7</td>
<td></td>
<td></td>
<td>High priority</td>
</tr>
<tr>
<td>Risk 5</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>7</td>
<td></td>
<td></td>
<td>High priority</td>
</tr>
<tr>
<td>Risk 6</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td>7</td>
<td></td>
<td></td>
<td>High priority</td>
</tr>
<tr>
<td>Risk 7</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>5</td>
<td></td>
<td></td>
<td>Medium priority</td>
</tr>
<tr>
<td>Risk 8</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td></td>
<td></td>
<td>Low priority</td>
</tr>
</tbody>
</table>

### Fuel slip
- **Risk 5**: A malicious insider with access to the computer that stores the fuel slip performs changes to the data contained in the fuel slip.

### Cargo assignment
- **Risk 6**: The attacker intercepts the fuel slip, changes the data contained and sends it to the supplier.
- **Risk 7**: A malicious insider with access rights performs changes to the cargo assignment document before it is sent to a service provider.
- **Risk 8**: An attacker hacks the airline mailing list, receives the cargo assignment, changes the data contained and sends the cargo assignment to a service provider.
Message to Take Home

If you do not measure – you do not control