DEEPSEC

Off-Shore Development and Outsourcing - Information Security in Plato's Cave

DeepSec 2010, Vienna

Frank Ackermann, Dipl.-Inf. (FH), CISSP

Disclaimer

- This talk does not contain proof of concepts, shell code, scripts or other in-depth technical details.
- The content of this talk does not reflect the opinion and security safety measures of my current or former employers.

whoami

- Working as an IT- and Information Security Specialist since over a decade, focused on Security Management, Consulting and Architecture.
- Living and working in Düsseldorf, Germany.
- upload: cissp@gmx.de

- lets start with the download...

Definition: Off-shoring and Outsourcing

Definition:

- Offshore = outside coastal waters, outside of someone's territory, outside of a field of applications. (e.g. power generator, windmills)
- Outsource = order services by another company or spin off tasks and/or information handling to an external supplier
- Off-shore development = projects or task of a project is outsourced to fill a gap (knowledge, manpower, budget)

Plato's Cave

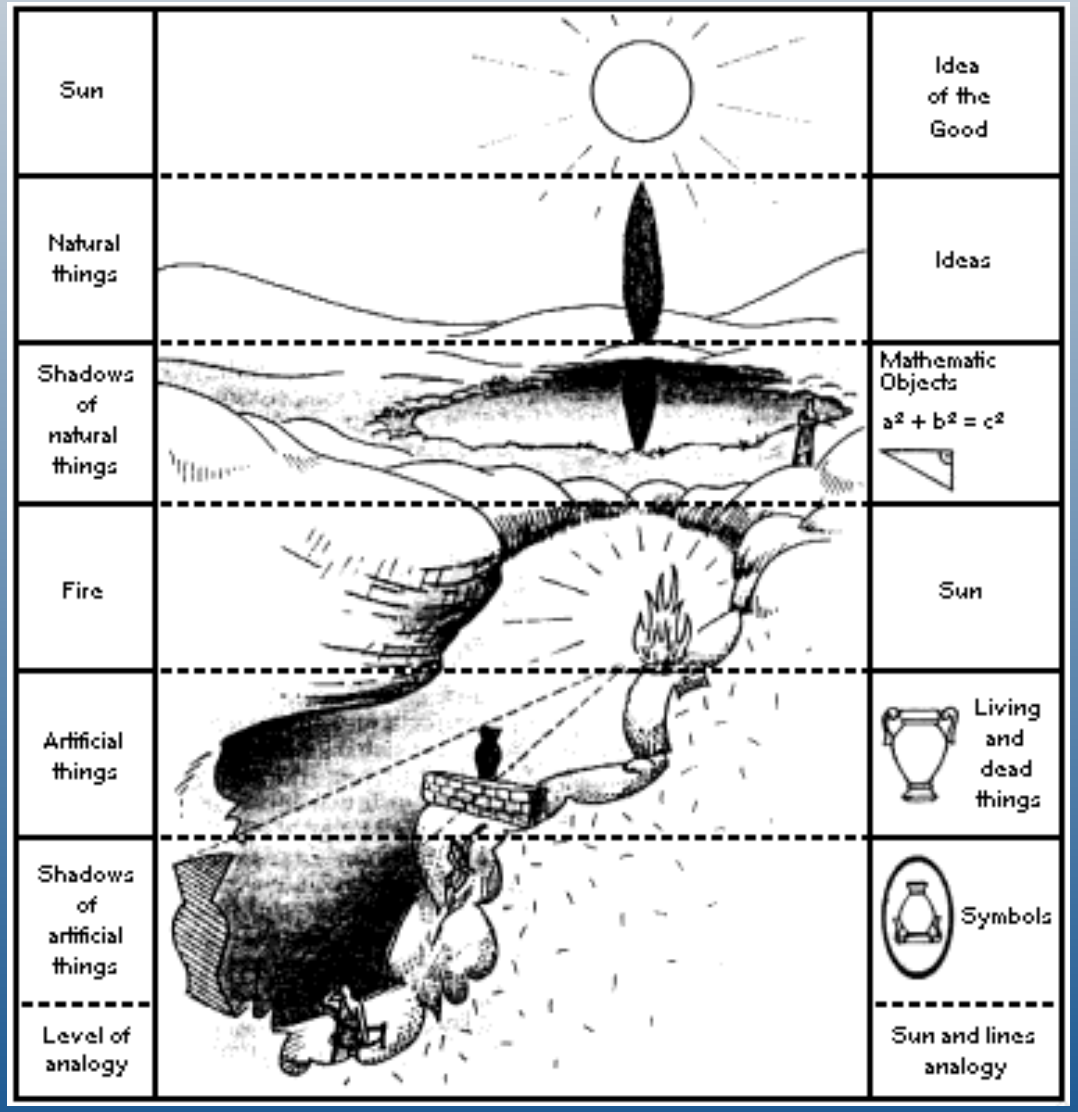
- The myth of the cave in Plato's allegory is about ideas, the truth and the interpretation of the real world.
- Summed up: Plato describes a group of people who are chained in a cave. These people interpret their reality and the real world only by looking at the shadows (created by the fire in the cave behind a wall).

Plato's Cave II

- Video
  „The Cave: An Adaptation of Plato's Allegory in Clay“, bullheadent
- http://www.youtube.com/watch?v=69F7GhASOdM

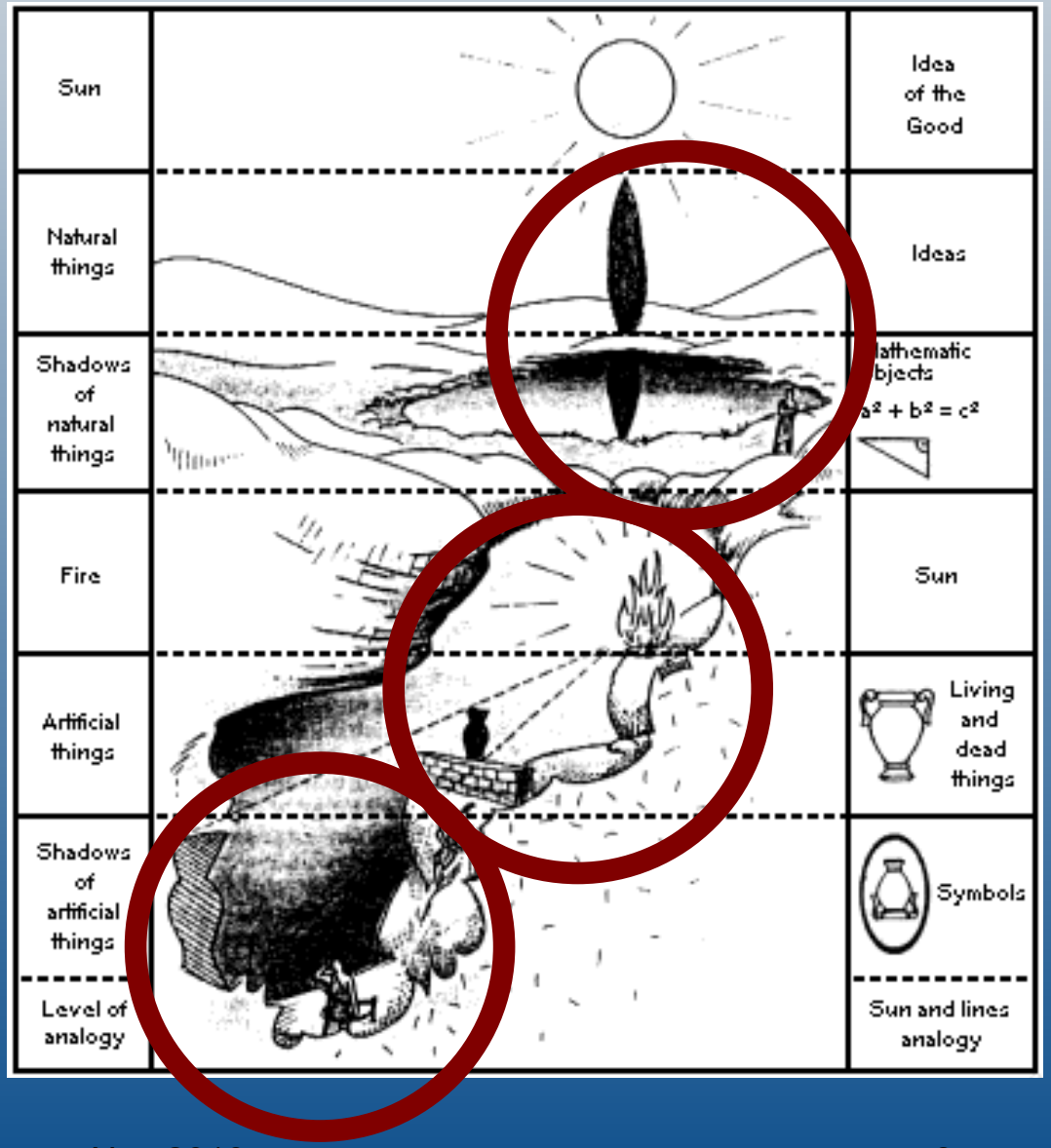
Plato's Cave III

- Possible viewpoints:
  - Chained and see the shadows
  - Free to understand the reason for the shadows
  - Free to go outside the cave
  - Be outside the cave and see the sun, which produces shadows by itself.
- Return to the cave?



Chain Information Security?

- Based on the allegory it is necessary to understand our viewpoint, describe the Off-Shore- and Outsourcing-Situation and think about the fire, the shadows and the sun.



Level of Analogy and the Shadows

- We are the prisoners.
- The chains are our interpretation of how we should implement security in the world.
- The shadows we see are our understanding how things might be. We generate our “real world”. (result of compliance checks, results of certifications)

The Artificial Things (Objects)

- The objects (things) that cast the shadows are visible to the man in front of the wall.
- Your supplier, outsourcer or Off-Shore-partner knows that he produces a shadow.
- He knows that this shadow produces a reality for the prisoners.
- He can modify the shadow - and the result of the compliance-check!

The Fire

- The fire is the rule set of the well-known compliance- and licensing-model.
- The fire defines a standard (light) and consistent reality within the cave.
- By not knowing the real-world one or more fire(s) are burning.
- The man and the objects (things) cannot modify the fire but modify the shadows.
- Compliance check: e.g.
  - SAS 70 report (I&II), ISO 270**, Company specific guidelines and reports, Company's maturity level, PCI DSS

The Real World I

- Outside the cave there is the real world:
  - Daylight
  - Shadows
  - Colours
- Speaking blunt:
  - information warfare & industry espionage
  - insider attacks
  - external intruders
  - 0dayz
  - vendor problems +++

The Real World II

- But there is also Good:
  - the understanding for security
  - people who would like to help
  - security evangelists.
- Even when the daylight hurts, after a process of adoption (by understanding the upper world), we realise the situation we are in.

Why Plato's Allegory? I

- We have been in the real world.
- We know the natural real objects and we understand the function of the sun.
- We have seen the daylight and know that there can be shadow.
- By thinking about and ordering off-shore development, outsourcing the IT and our information (without a concrete strategy) we knowingly chain us again deep deep in the cave.

Why Plato's Allegory? II

- We do not control the fire and need to trust the men who cast the shadows.
- We have to trust the fire makers and the persons who define the rules for the fire and the casted shadows.
- We can't change the cave.

Lets Go into the Cave I

- Types of Off-shoring and outsourcing:
  - buy extra time-limited resources and know-how (e.g. consulting)
  - IT hosting (e.g. cloud services)
  - development
  - source out IT parts of the company (e.g. IT project management or HR ;-)
  - total IT (partnering)

Lets Go into the Cave II

- Reasons:
  - build something new on flex-men-power
  - get rid of people
  - get rid of IT (because it's no core business)
  - hidden agenda
- And always:
  - Talking about money ... like ROSI (Return on security investment) ;-)

How Does the Cave Look Like?

- We have been outside the cave, know the “real world” and now decide (based on any decision) to order outsourcing or off-shoring
- We sit in the cave and hardly try to interpret the shadows
- These shadows will be our “new” “real world”.

Major Difference to Plato's Prisoners

- The prisoners (we) know that they (we) are sitting in a cave
- They (we) can (more or less) talk to the men and objects that casts the shadows
- We can change the situation!
- Result:
  - You can ask for your images and 'world- information'
  - But how? Ahhhh yes – Standards!

Of Course We Have Baselines and Standards!

- (Industry) Standards: e.g.
  - SAS 70 I&II report
  - ISO 270**
  - COBIT
  - PCI DSS
  - … and others.
- You and your partners have baselines too!
  - Company specific security guidelines
  - development guidelines
  - individual compliance checks
  - companies maturity levels

The Surrounding

- National laws:
  - local national law
  - group / company policy
  - if EU -> EU law-set
  - International non-EU law- set
  - Data-protection law EU / non-EU
  - Cross border-transfer (regulations) of (for) information
  - Cross border encryption policy / laws (e.g. limitation and definition for China, France, USA)
- Language problems
- Cultural problems

Risks and Benefits

- You are willed to put yourself in the position
- You start to over-think aspects of your (core) business, your IT, your budget - are there any risks? We should talk about chances!
- Confidence = trust + control
- Confidence = trust + control + acceptance of residual risks

Benefits

- You are flexible
- Your can extend and increase your know-how level
- You can extend your business by in / source out certain aspects
  (e.g. online-shops + delivery)

Risks – IT Partnering (total IT)

- Data loss
- Loss of control and evidence
- Loss of architectural influences
- Blending of partner's client data (your supplier mixed up data of his clients)

Risks – Source Out (parts)

- Loss of company data
- Loss of knowledge
  (e.g. concerning project information)
- Loss of application and business knowledge

Risks – Support and Consulting

- Knowledge transfer
- Information loss
- Re-use of results
- Integrity and confidentiality

Risks – Development

- Intellectual property + copyrights
- Local admin rights
- Development equipment
- Data & Source code loss
- Malicious code in source code or binary
- Open source code in closed source code (license and security)
- Re-use of code snippets (more than one company)
- Information and source code flows out and into your company (… test data ...)

Risks – Other Aspects

- Data exchange (transmission and connection)
- Virtual equipment used by your partner
- Intellectual property and copyright aspects
- Sub-contractors (off-shore the off-shore)

- YOU ARE THE ASSET OWNER!
- IT IS (Y)OUR REPUTATION!

Protect Your Cave!

- How to mitigate the risks?
- We know the risks
- We know we can be manipulated

Mitigation – Strategy, Strategy, Strategy!

- It is always the same - you have to over-think what you want (to achieve) and what your target is!
- A strategy must be defined - before you handshake “the deal” at the golf course!
- The strategy must include a business strategy, an IT strategy and (!!!) an IT/Information security strategy!
- ➔Know what you order!

Mitigation – Information Security Aspects

- Classify your business and workflow's
- Classify your data
- Asset and risk classification/analysis is necessary
- Limit access to data
- Revise your access controls
- Over-think the controls
- Know your information-flow

Mitigation – Audit and Compliance

- Develop a security guideline (based on your security strategy) to describe how you would like to proceed
- Define very clearly what you expect and what kind of evidence (result and quality) you would like to see!
- (audit proof and evidence)
- Define ways to handle incidents
- Audit by yourself (do not expect that the man casting the shadows has the same understanding of shadows)

Mitigation – Network And Connection

- Generate segregated networks / isolated networks
- Define information flow and exchange possibilities
- Over think your entry points (in-going connectivity's, exchange of data)

Mitigation – Sourcing, Law & Regulations I

- Define security issues in the Request For Proposal (RFP)
- Avoid promises; do it, fix it!
- Bind externals with a concrete contract
- Revise and verify your sourcing strategy
- Check your sourcing and ordering process

Mitigation – Sourcing, Law & Regulations II

- Define non-negotiable contract-parts which contain
  - intellectual property
  - copyright
  - local / national law
  - data protection law
  - penalty aspects
  - direct links to your security guideline

Mitigation – Development and Architecture

- Work on your virtualisation concept
- Over think and revise the local admin concept
- Run security and quality checks on the source code
- Specify controls and audit's in development

Who can help?
Outsource the Outsource!

- Why get dirty hands? Ask professional support for offshore development and IT-Outsourcing!
- Companies offer full engagement, services and consulting to support your outsourcing.
- Supporter-Managed ODCs vs. Client-Managed ODC

Who can help? Outsource the Outsource! II

Example: Achievo's professional services team provides in-depth research on locations, including city proles that cover:

- Transportation
- Local talent pool
- Long-term client strategy
- Infrastructure
- Political and economic environment
- Culture, lifestyle and living conditions
- Consult Consult Consult
- Location Location Location
- +++
- Figure: http://www.achievo.com/upload_file/Achievo-Offshore-Development-Center-Brochure-2009-01-19-EN.pdf

Catalog	Service Items	Client Managed ODC		Achievo-Managed ODC	
		Achievo	Client	Achievo	Client
Facility Management	Furniture maintenance	x		x	
	Computer maintenance	x		x	
	Network equipment	x		x	
	Conference / other equipment	x		x	
IT & IP Protection	Internet and intranet	x	x	x	
	Physical security	x	x	x	
	Data security and back-up		x	x	
	Disaster recovery		x	x	
	Software maintenance		x	x	
	Intrusion detection		x	x	
	Antivirus		x	x	
	Document management		x		
Operations Support	Accounting support	x		x	
	Procurement support	x	x	x	x
	Timesheet and billing	x	x	x	x
	Administrative support	x		x	
	Legal support	x		x	
Staffing, HR and Training	Recruiting and hiring	x	x	x	
	Labor contracts	x		x	
	Orientation and training	x	x	x	
	Retention program	x	x	x	
	Salary, insurance, benefits	x		x	
	Specific talent pool maintenance	x		x	
Process and Project Management	Process management		x	x	
	Project management		x	x	
	Quality assurance management		x	x	
	Communications management		x	x	
	Source Code management		x	x	

Figure 4: Achievo ODC services menu

Who can help?
Outsource the Outsource! III

- As-is-situation:
  Business ➔ (orders) ➔ IT
- New situation:
  Business ➔ (orders) ➔ *IT* + Outsourcer / Supplier / external partner
- “Supported” situation:
  Business ➔ (orders) ➔ *IT* + Outsourcing-supporter ➔ (orders) ➔ Outsourcer/Supplier/external partner
- This helps! ;-)
- BTW: Ramp up-service offered … but no shut down service.

Conclusion and Summary

- You are responsible for your business; even when you are ordering a contractor.
- You know what the real world looks like.
  - Return to the fire? Return to the cave?
- By ordering real-world images casted in the cave, high endeavours have to be made!
- To stay in the cave you have to invest in protecting mechanisms!
- It is required to do a comprehensive analysis before starting with this topic.

Questions?

- Thank you for your attention
- Any questions?

BTW: Do you do offshore banking? ;-)

Merry Christmas!

http://forums.justcommodores.com.au/attachments/jokes-humour/29100d1161834356-outsourcing-santa-christmas.jpg

Links, Information, Sources

- “The Security Challenges of Offshore Development”, SANS Institute, InfoSec Reading Room, 2001
- http://www.offshoringtimes.com/Pages/2006/offshore_news496.html
- http://www.achievo.com/upload_file/Achievo-Offshore-Development-Center-Brochure-2009
- http://www.platon42.de/caveanalogy.html
- http://en.wikipedia.org/wiki/Allegory_of_the_Cave
- http://rzbl04.biblio.etc.tu-bs.de:8080/docportal/servlets/MCRFileNodeServlet/DocPortal_de
- http://www.capurro.de/plato.html