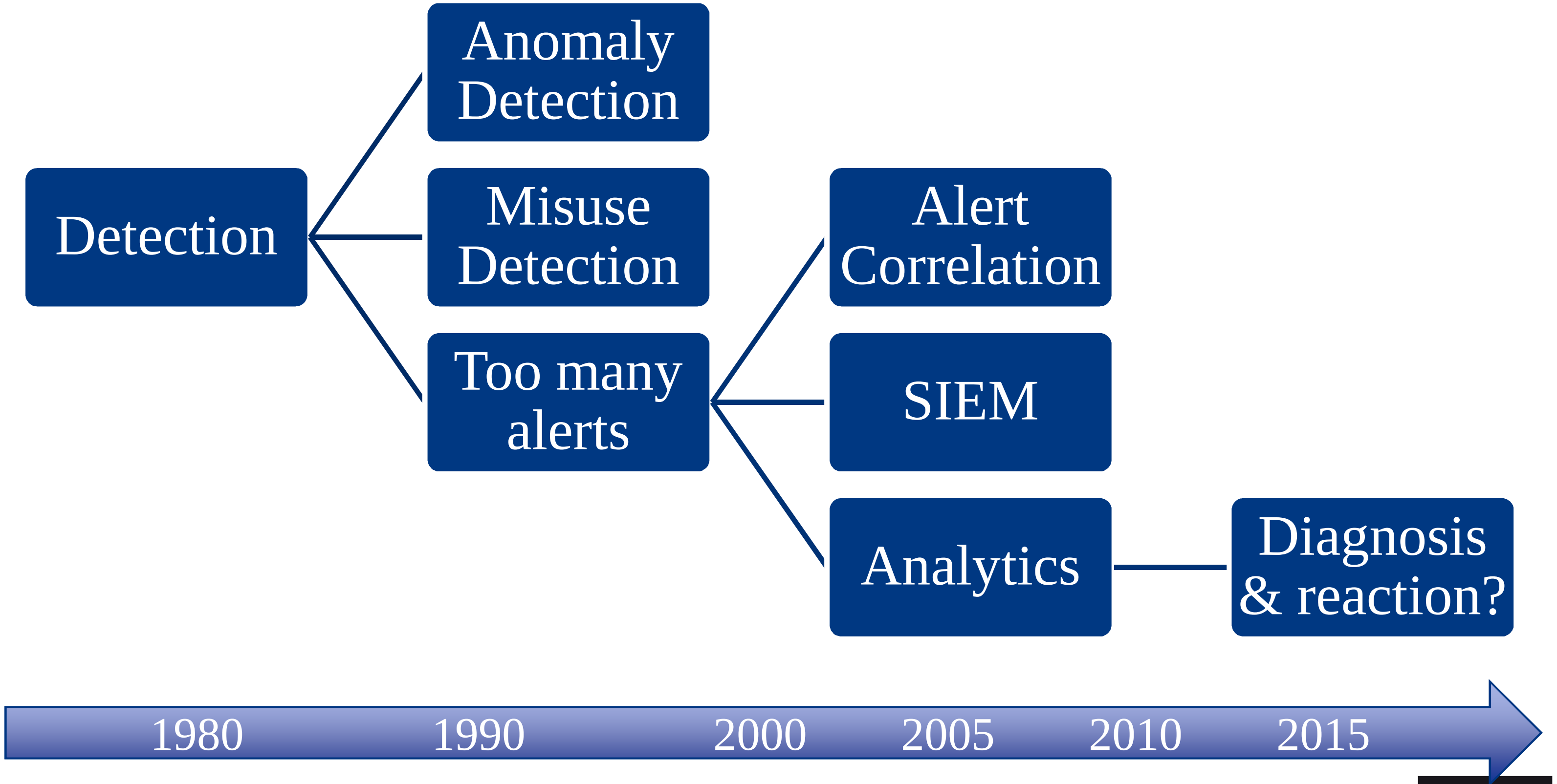
Institut
Mines-Télécom

Towards a Quantitative Approach to Attack Response

Hervé Debar

Using work performed during the PhD theses of Yohann Thomas, Nizar Kheir, Gustavo Gonzalez-Granadillo

« Operational security » timeline



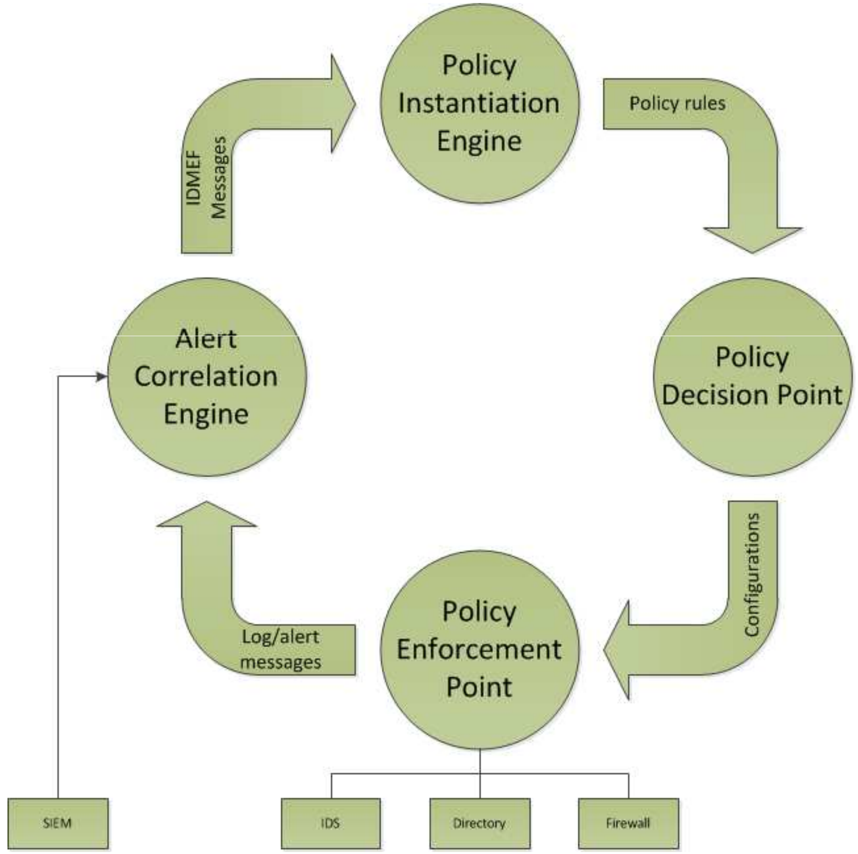
TELECOM SudParis

Reaction models

- **Alert-triggered**
  - Network-based
    - Reset connection, block flow, …
  - System-based
    - Kill process, disable account, …
  - Independant actions, repeated for each and every alert
    - Marginal improvement with integration in the Bro framework[RAID2015]
- **Policy-triggered**
  - Workflow
    - Select appropriate rule
    - Deploy rule
- **Issues**
  - Multiple attacks
  - Continuous operation

Dynamic reaction model

- **Feedback control loop [Thomas et al. 2007]**
  - Definition of a contextual security policy
  - Contexts are influenced by IDMEF messages
  - Deployed policies adjust configuration to attack
- **Pros**
  - Dynamic adjustment of posture
- **Issues**
  - Pre-registration of contexts, one per CVE
  - Finding PEPs
  - Conflict management
    - Programmatic context combination



Finding the right PEPs

- **Problem: given a set of PEPs, which one is the best suited to handle an alert ?**
  - Capability
    - In transit
      - Network (block, kill connection, …)
      - System (kill process
    - In acces
      - Authentication (directories, …)
      - Communication (DHCP address, …)
  - Geography
    - Will the PEP intersect with the malicious activity ?
- **Proposal [Kheir 2010]: service dependency model**
  - AADL (hierarchical) provide-require interfaces
  - Down-the-chain: find appropriate PEP
  - Up-the-chain: find collateral damages

Challenges going forward

- **How to select an appropriate countermeasure from a group of candidates?**
  - Qualitative, quantitative or a combined approach?
  - Which parameters to consider in the evaluation of security solutions?

- **Once a countermeasure is selected, is it possible to combine it with other solutions?**
  - How to calculate the combined countermeasure cost?
  - How to calculate the combined mitigation level?

- **How to manage problems when proposing a solution that generates conflicts on the system?**
  - What to do when solutions are mutually exclusive?

- **How to select optimal solutions for a multiple attack scenario?**
  - How to calculate the combined attack surface?
  - One solution or a combined solution for a multiple attack?

Cost Sensitive Models

Models	Return On Investment (ROI)	Return On Attack (ROA)	Return On Security Investment (ROSI)	Return On Response Investment (RORI)
Main Focus	Security Effectiveness	Attacker's behaviour	Security Solution Benefits and Cost	Collateral Damage and Response Effects
Formula	$\frac{Benfits-Cost}{Cost}$	$\frac{AttackGain}{Cost_{BeforeSecurity}+Loss}$	$\frac{ExpectedReturns-InvestCost}{InvestCost}$	$\frac{ExpectedReturns-OperCost}{SolutionCost+OperCost}$
Optimal Solution	Highest ROI value	Lowest ROA value	Highest ROSI value	Highest RORI value
Characteristics	Evaluate financial consequences of business investments	Evaluate the impact of security solutions based on the attack's behaviour	Compare the difference between damages of IT incidents (with and without countermeasures) against the cost of the solution	Determine the percentage of benefit that can be obtained in a particular threat scenario that applies a given countermeasure
Constraints	It cannot be used to evaluate the fact of doing nothing	Difficult to be accurate while predicting attacker's behaviour	It does not consider collateral damage nor operational costs	It does not consider attacker's behaviour
	Unable to catch different impact that solutions may have on attacker's behaviour	It does not consider security solution cost	It cannot be used to evaluate the fact of doing nothing	Unable to evaluate the solution's impact due to attacker's behaviour
	It does not consider collateral damage nor operational costs	It cannot be used to evaluate the fact of doing nothing	Unable to evaluate the solution's impact due to attacker's behaviour	

TELECOM SudParis

Initial Return On Response Investment (RORI) Index

$$\text{RORI} = \frac{(\text{ICb} - \text{RC}) - \text{OC}}{\text{CD} + \text{OC}} \times 100$$

Kheir et al.

Where

ICb→ Intrusion Impact in the absence of security measures.

RC→ Combined Impact for both intrusion and response.

CD→ Response collateral damage (cost added by the countermeasure).

OC→ Operational cost that includes response set-up and deployment costs.

Constraints

- The absolute value of **ICb** and **RC** are difficult to estimate.
- Evaluation of doing nothing.
- RORI is not normalized to the size and complexity of the infrastructure

TELECOM SudParis

Countermeasure Selection Model (1/2)

Improved Return On Response Investment

$$RORI = \frac{(ALE \times RM) - ARC}{ARC + AIV} \times 100$$

Fixed Parameters

Annual Loss Expectancy (ALE) → Impact Cost in the absence of countermeasures (e.g., $/year).

Annual Infrastructure Value (AIV) → Fixed costs regardless of the implemented CMs (e.g., $/year).

Variable Parameters

Risk Mitigation (RM) → Percentage of reduction of the total incident cost after the implementation of a countermeasure

Annual Response Cost (ARC) → costs associated to a given countermeasure (e.g., $/year).

Countermeasure Selection Model (2/2)

Improved Return On Response Investment

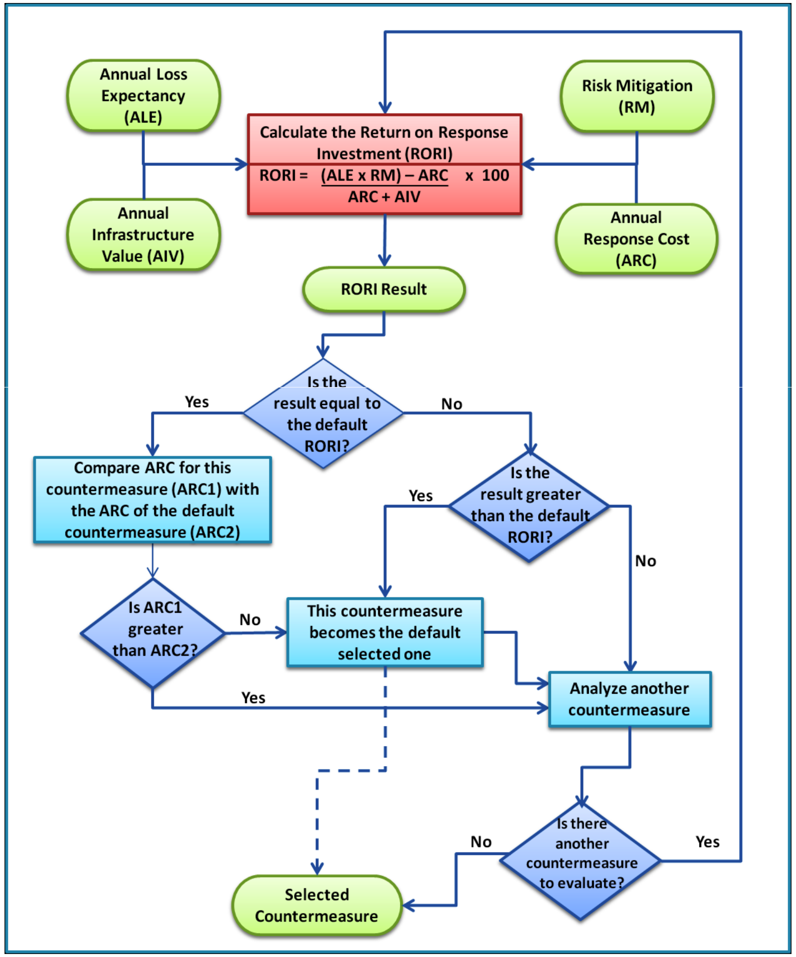
$$\textbf{RORI} = \frac{(\textbf{ALE x RM}) - \textbf{ARC}}{\textbf{ARC} + \textbf{AIV}} \textbf{ x 100}$$

Improvements

- ✓ The ICb – RC parameters are substituted by ALE x RM, which reduces error magnitude.
- ✓ The introduction of AIV handles the case of selecting no countermeasure.
- ✓ The AIV provides a response relative to the size of the infrastructure.

ALE: Annual Loss Expectancy
AIV: Annual Infrastructure Value
RM: Risk Mitigation
ARC: Annual Response Cost

Countermeasure Selection Process



- **Limitations**
  - Accuracy in the estimation of the different RORI parameters.
  - The process does not consider inter-dependence among countermeasures.
  - RORI does not discusses restrictions or conflicts between countermeasures.
  - RORI limits the action of only one countermeasure over a given attack.

ALE: Annual Loss Expectancy
AIV: Annual Infrastructure Value
RM: Risk Mitigation
ARC: Annual Response Cost

Sensitivity Analysis (1/3)

$$RORI = \frac{(ALE \times RM) - ARC}{ARC + AIV} \times 100$$

Worst Scenario
ALE x RM << ARC

$$\frac{-ARC}{ARC + AIV}$$

Perfect Mitigation
RM = 1, ARC=0

$$\frac{ALE}{AIV}$$

If ALE x RM = ARC → RORI = 0
If ALE x RM < ARC → RORI < 0
If ALE x RM > ARC → RORI > 0

ALE: Annual Loss Expectancy
AIV: Annual Infrastructure Value
RM: Risk Mitigation
ARC: Annual Response Cost

Sensitivity Analysis (2/3)

Main Results

$$RORI = \frac{(ALE \times RM) - ARC}{ARC + AIV} \times 100$$

ARC vs. AIV

If ARC << AIV → RORI ≅ ALE x RM / AIV — **Weak**

If ARC >> AIV → RORI ≅ (ALE x RM) – ARC / ARC — **Strong**

ALE vs. AIV

If ALE << AIV → RORI ≅ – ARC / ARC + AIV — **Negative**

If ALE >> AIV → RORI ≅ (ALE x RM) – ARC / ARC — **Positive**

ALE: Annual Loss Expectancy
AIV: Annual Infrastructure Value
RM: Risk Mitigation
ARC: Annual Response Cost

Sensitivity Analysis (3/3)

Main Results

$$RORI = \frac{(ALE \times RM) - ARC}{ARC + AIV} \times 100$$

ALE vs. ARC

If ALE << ARC → RORI $\cong$ – ARC / ARC + AIV — **Negative**

If ALE >> ARC → RORI $\cong$ ALE x RM / AIV — **Positive**

Risk Mitigation (RM)

If RM increases → RORI $\cong$ ALE – ARC / ARC + AIV — **Positive**

If RM decreases → RORI $\cong$ – ARC / ARC + AIV — **Negative**

ALE: Annual Loss Expectancy
AIV: Annual Infrastructure Value
RM: Risk Mitigation
ARC: Annual Response Cost

Multiple counter-measures ?

We do not go from 0 to 1, but from n to n+1

TELECOM SudParis

How to combine two or more countermeasures?

- **Annual Response Cost (ARC)** → **ARC = ∑ (direct cost + indirect cost)**
- **Risk Mitigation (RM)** → **RM = Surface Covered x Efficiency**

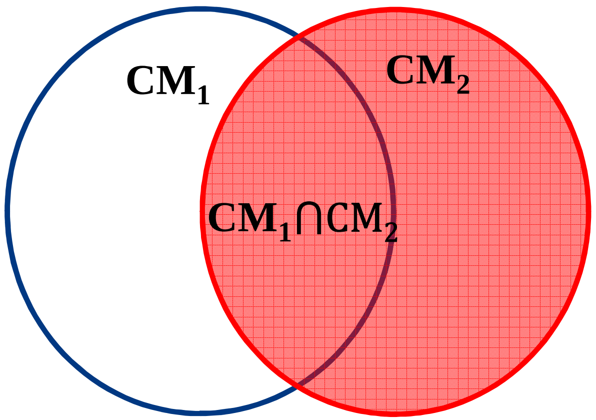
No exact values → Approximations

Optimistic	Pessimistic	Average
$ARC(CM_1 \cup CM_2) = \max\{ARC(CM_1), ARC(CM_2)\}$	$ARC(CM_1 \cup CM_2) = ARC(CM_1) + ARC(CM_2)$	$ARC(CM_1 \cup CM_2) = \frac{ARC(CM_1) + ARC(CM_2)}{2}$
$RM(CM_1 \cup CM_2) = RM(CM_1) + RM(CM_2)$	$RM(CM_1 \cup CM_2) = \max\{RM(CM_1), RM(CM_2)\}$	$RM(CM_1 \cup CM_2) = \frac{RM(CM_1) + RM(CM_2)}{2}$

Combinatorial Axioms

Axiom 1: The cost of a combined countermeasure is equal to the sum of all individual countermeasure's cost.

$$ARC(C_1 \cup C_2) = ARC(C_1) + ARC(C_2)$$



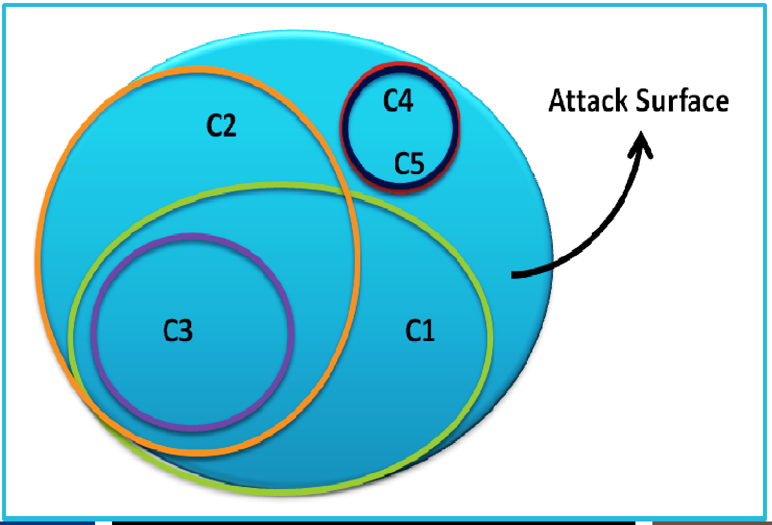
Axiom 2: The risk mitigation (RM) for a combined solution is calculated by adding the effectiveness (EF) of countermeasures over the different surfaces they cover (SC) minus their intersection.

$$RM(C_1 \cup C_2) = SC(C_1) \times EF(C_1) + SC(C_2) \times EF(C_2) - SC(C_1 \cap C_2) \times \min\{EF(C_1), EF(C_2)\}$$

$$SC(C_1 \cap C_2) = \frac{SC(C_1 \cap C_2)_{MIN} + SC(C_1 \cap C_2)_{MAX}}{2}$$

Attack surface

- **Software-oriented definition**
  - LoC
  - Intersection == common code
- **Does not really work for our purpose**



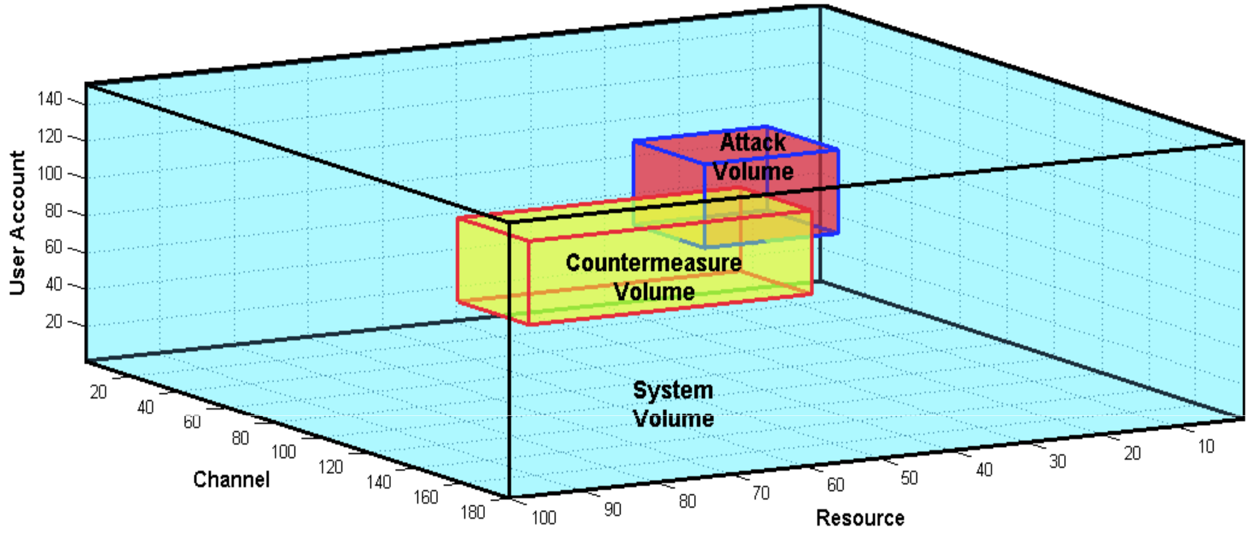
- **What we need to model:**
  - Set definition
  - Multiple countermeasures
  - Non-restrictive, Partially restrictive, Totally restrictive
  - Joint vs. Disjoint countermeasures
  - Countermeasure Overlap
- **Countermeasure Union & Intersection**
  - - > Attack volume

TELECOM SudParis

Coordinate System

Access Control

Subject
Action
Object



System Volume, which represents the maximal space to which a given system (e.g. S1) is exposed to be attacked.
Attack Volume, which represents a portion of the system volume that is vulnerable to a given attack (e.g. A1).
Countermeasure Volume, which represents the portion of the system volume that is mitigated by a given countermeasure (eg. CM1).

Inter-dimension Weighting Factor

Dimension-based Weighting Factor

Attack Dimension	C	A	R	V	E	R	Total	%	Weight Factor
User Account	8	7	9	7	8	7	46	40%	2
Channel	5	6	5	6	5	4	31	28%	1
Resource	7	6	6	5	7	5	36	32%	1.5

C-Criticality, A-Accessibility, R-Recuperability, V-Vulnerability, E-Effect, R-Recognizability

Volume Calculation

$SV(S1) = Co_{Acc}(S1) \times 2 \times Co_{Ip\text{-}Port}(S1) \times 1 \times Co_{Res}(S1) \times 1.5$

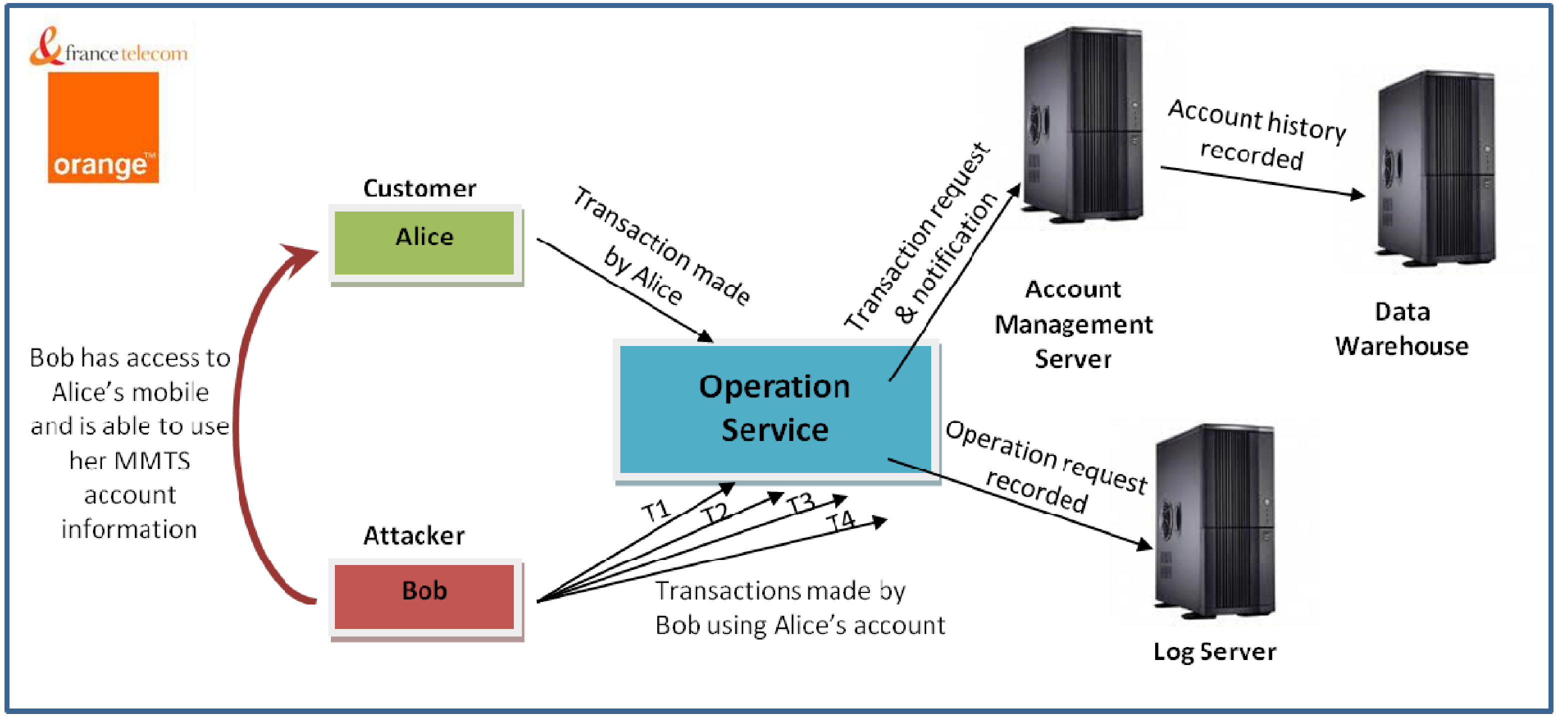
$AV(A1) = Co_{Acc}(A1) \times 2 \times Co_{Ip\text{-}Port}(A1) \times 1 \times Co_{Res}(A1) \times 1.5$

$CV(C1) = Co_{Acc}(C1) \times 2 \times Co_{Ip\text{-}Port}(C1) \times 1 \times Co_{Res}(C1) \times 1.5$

Use case (Orange): Mobile Money Transfer Service

TELECOM SudParis

Use Case: Mobile Money Transfer System (1/5)



Severity: Minor = 100 €
Likelihood: High = 12 times/year

ALE = 1200 €/year

TELECOM SudParis

Use Case: Mobile Money Transfer System (2/5)

Annual Infrastructure Value (AIV)

	PEP	Type	AIV	Threats that mitigate							
				T1	T2	T3	T4	T5	T6	T7	T8
E1	Intrust	HIDS	800€	✓		✓					✓
E2	Tripwire	HIDS	250€	✓		✓					✓
E3	Verisys	HIDS	400€	✓		✓					✓
E4	Snort	NIDS	400€	✓	✓	✓	✓	✓	✓	✓	✓
E5	NetCrunch	Net. Monitoring	1500€	✓	✓	✓	✓	✓	✓	✓	✓
E6	FreeNATS	Net. Monitoring	500€	✓	✓	✓	✓	✓	✓	✓	✓
E7	Comodo	Firewall	300€	✓	✓	✓	✓		✓		✓
E8	Endian	Firewall	150€	✓	✓	✓	✓		✓		✓
E9	Cisco SA 500 series	IPS	1000€	✓	✓	✓	✓	✓	✓	✓	✓
E10	Kaspersky	Antivirus	300€						✓		✓
E11	OS update	OS Hardening	500€				✓		✓		✓
E12	Software Token	Auth. Method	400€	✓	✓	✓	✓	✓	✓	✓	

T1 Trafficking Collection
T2 Hiding User Identity
T3 Scams
T4 Account Takeover
T5 Employee Complicity
T6 Denial of Service
T7 Money Creation/Destruction
T8 Other threats (e.g. malwares, virus)

AIV= 2,600 €/year

TELECOM SudParis

Use Case: Mobile Money Transfer System (3/5)

Countermeasure Evaluation

C1 Do Nothing: Accept the risk and does not perform any modifications. The cost and risk mitigation level are equal to zero.

C2 Deny Transaction: Allow the user to authenticate but he/she is not able to perform any kind of transaction.

C3 Deactivate User Account: Temporarily deactivation of the user account (e.g., for a period of 24, 48 or 72 hours).

C4 Reduce Transaction Amount: Limit suspected user accounts to perform transactions for a maximum amount of money (e.g., up to 30$, 50$, 100$).

C5 Reduce Number of Transactions: Limits the user to perform a controlled number of transactions per day (e.g., 2, 3, or 5 transactions per day).

Use Case: Mobile Money Transfer System (4/5)

Countermeasure Evaluation

C6 Active Alert Mode: An alert indicates that the denied user account is suspected to be under attack.

C7 Keep the Account under Surveillance: The user account is taken into quarantine in order to punctually block operations.

C8 Activate Two-factor Authentication: Requests an additional authentication (e.g., passphrase, challenge response, PIN), in order to authorize the user to perform the required transaction.

C9 Deactivate Multiple Transaction Requests: Limit the user to emit only one transaction at a time.

Use Case: Mobile Money Transfer System (5/5)

Combined Countermeasure Evaluation

Countermeasure	PEP	RM	ARC	RORI
C1. Do nothing	-	0%	0€	0,00%
C2. Deny transaction	E7	72%	60€	30,34%
C3. Deactivate user account	E9	68%	55€	28,66%
C4. Reduce transaction amount	E4	60%	50€	25,77%
C5. Reduce number of transactions	E4	53%	30€	22,81%
C6. Activate alert mode	E4	42%	25€	18,25%
C7. Keep account under surveillance	E9	42%	40€	17,58%
C8. Activate multi-factor authentication	**E12**	**77%**	**50€**	**32,75%**
C9. Deactivate multi-trans. requests	E9	64%	20€	28,55%

Optimal Countermeasure: Activate Multiple Factor Authentication (C8)

Individual Countermeasures Analysis

Example: Account Takeover Attack in the MMTS

Countermeasure	RM	ARC	RORI	Restriction
C1. NOOP	0%	0€	0.00%	Totally rest.
C2. Deny transaction	72%	60€	30.34%	Totally rest.
C3. Deactivate user account	68%	55€	28.66%	Totally rest.
C4. Reduce transaction amount	**60%**	**50€**	**25.77%**	**Non-restrictive**
C5. Reduce number of transactions	**53%**	**30€**	**22.81%**	**Non-restrictive**
C6. Activate alert mode	42%	25€	18.25%	Non-restrictive
C7. Keep account under surveillance	42%	40€	17.58%	Non-restrictive
C8. Activate multi-factor authentication	**77%**	**50€**	**32.75%**	**Non-restrictive**
C9. Deactivate multi-trans. requests	**64%**	**20€**	**28.55%**	**Non-restrictive**

Source: France Telecom Orange Labs

RORI Average = 22.66%

TELECOM SudParis

Combined Countermeasure Evaluation

Countermeasure	ARC	SC	EF	RM	RORI
C4	35€	0.70	0.75	0.53	25.77%
C5	30€	0.70	0.85	0.60	22.81%
C8	50€	0.85	0.90	0.77	32.75%
C9	35€	0.80	0.80	0.64	27.82%
C4 & C5	65€	0.55	0.75	0.71	29.42%
C4 & C8	**85€**	**0.63**	**0.85**	**0.83**	**33.87%**
C4 & C9	70€	0.60	0.80	0.76	31.31%
C5 & C8	80€	0.63	0.75	0.82	33.79%
C5 & C9	65€	0.60	0.75	0.72	29.76%
C8 & C9	85€	0.73	0.80	0.83	33.71%
C4 & C5 & C8	115€	0.48	0.75	0.83	32.39%
C4 & C5 & C9	100€	0.45	0.75	0.76	29.85%
C4 & C8 & C9	120€	0.53	0.80	0.83	32.15%
C5 & C8 & C9	115€	0.53	0.75	0.83	32.23%
C4 & C5 & C8 & C9	150€	0.38	0.75	0.83	30.71%

C4: **Reduce Transaction Amount**
C5: **Reduce number of transactions**
C8: **Activate Multiple Factor Authentication**
C9: **Deactivate multiple transaction request**

Source: France Telecom Orange Labs

TELECOM SudParis

Use case 2: IT system@Telecom SudParis

TELECOM SudParis

Use Case: Telecom SudParis

System Volume

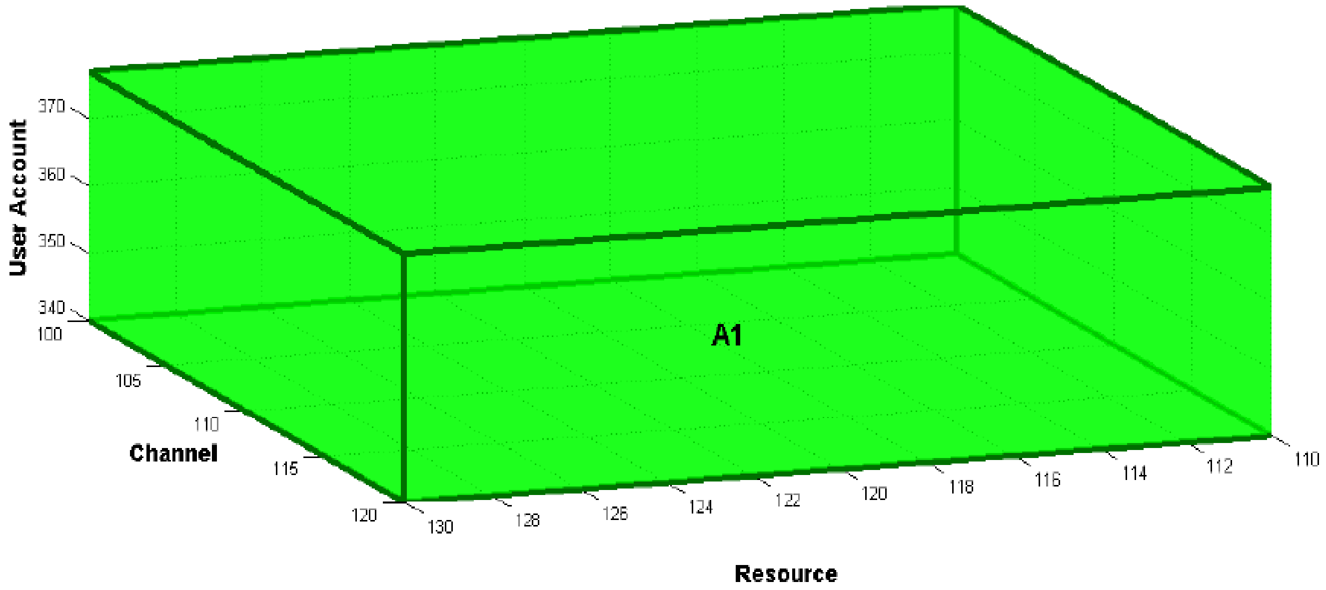
Dimension	Range	Description	Quantity	Weight Factor
User Account	U1:U263 U264:U428 U429:U633 U664:U3721	Super admin System admin Standard user Internal user	263 165 205 3058	4 3 2 1
Channel	Ch1:Ch4500 Ch4501:Ch4512	Active public IP Port Class 1	4500 12	3 3
Resource	R1:R40 R41:R43 R44:R93 R94:R993	Kernel&WRX Kernel&WR/WX/RX Kernel&W/X User&WRX, User&WR/WX/RX, Kernel&R	40 3 50 900	5 4 3 2

SV(S1) = 430,106,901,440 units^3

Attack 1: Zeus

Attack Volume

Targets:
U340:U377
Ch100:Ch120
R110:R130



Zeus Infection

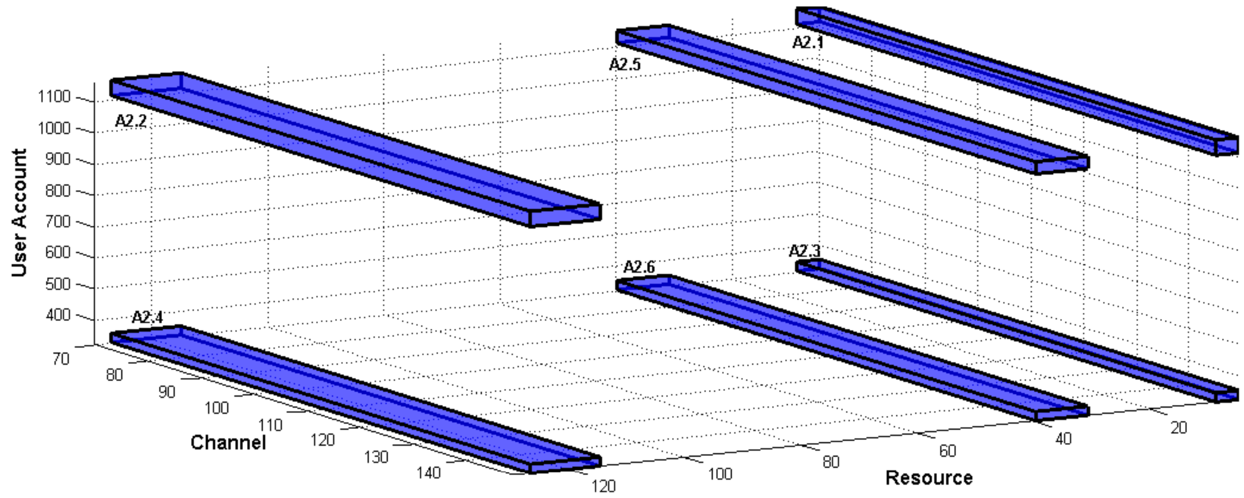
AV(A1) = [(38x3)x2] x [(21x3)x1] x [(21x2)x1.5]
AV(A1) = 904,932 units^3

C(A1)/(S1) = 0.0002%

TELECOM SudParis

Attack 2: Conficker

Attack Volume



Targets:
U320:U349 & U1110:U1159
Ch70:Ch149
R5:R9 & R31:R40 & R115:R12

Conficker Infection

AV(A2.1) = [(50x1)x 2] x[(80x3)x1]x [(5x5)x1.5] = 900,000 units^3
AV(A2.2) = [(50x1)x 2] x[(80x3)x1]x [(13x2)x1.5] = 936,000 units^3
AV(A2.3) = [(30x3)x 2] x[(80x3)x1]x [(5x5)x1.5] = 1,620,000 units^3
AV(A2.4) = [(30x3)x 2] x[(80x3)x1]x [(13x2)x1.5] = 1,684,800 units^3

Conficker DB Brute Forcing

AV(A2.5) = [(50x1)x 2] x[(80x3)x1]x [(10x5)x1.5] = 1,800,000 units^3
AV(A2.6) = [(30x3)x 2] x[(80x3)x1]x [(10x5)x1.5] = 3,240,000 units^3

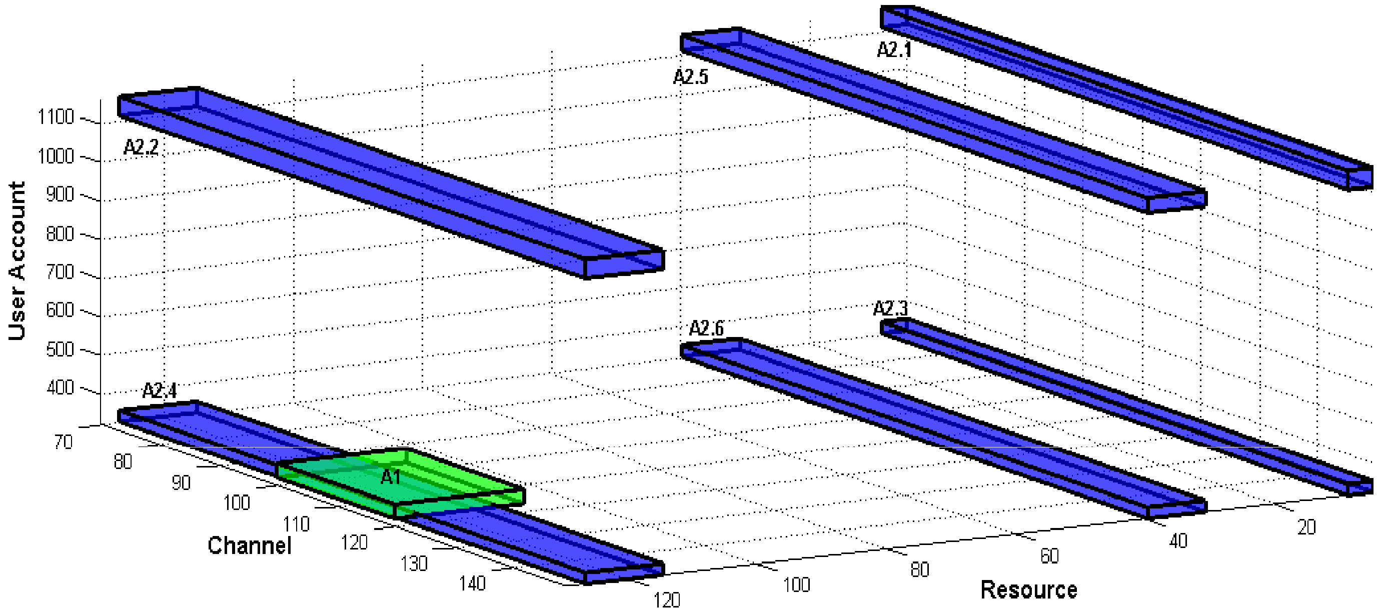
AV(A2) = 10,180,800 units^3

TELECOM SudParis

Combined Attack: Zeus & Conficker

Attack Volume

Intersection Targets :
U340:U349
Ch100:Ch120
R115:R127



AV (A1 ∩ A2) = [(10x3)x2] x [(21x3)x1] x [(13x2)x1,5]
AV (A1 ∩ A2) = 147,420 units³

AV(A1∪A2) = 904,932units³ + 10,180,800units³ – 147,420units³
AV(A1∪A2) = 10,938,312units³

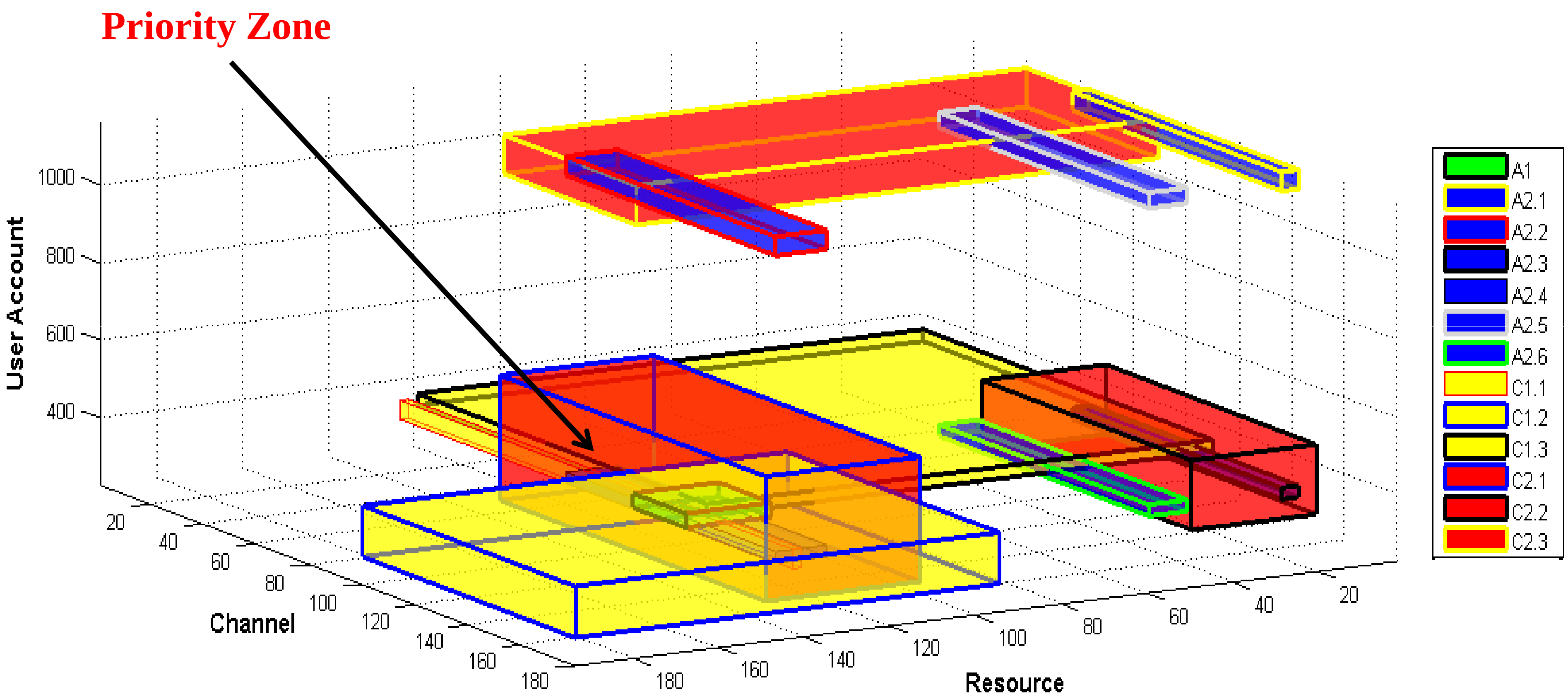
TELECOM SudParis

Countermeasure Volume

Countermeasure Information

Counter-measure	Description	User Account	Channel	Resource	Volume (units³)	Coverage (units³)
C1.1	Behavioral detection	U300:U349	Ch1:Ch149	R121:R123	1,206,900	388,800
C1.2	Antivirus	U301:U433	Ch100:Ch179	R94:R193	57,456,000	3,288,600
C1.3	Make all shares “read only”	U330:U360	Ch1:Ch110	R1:R119	25,411,320	3,260,115
C2.1	Install patches	U229:U550	Ch50:Ch110	R94:R130	35,124,840	2,696,652
C2.2	Block domains	U270:U449	Ch70:Ch149	R1:R30	56,052,000	3,132,000
C2.3	Create signatures	U1030:U1130	Ch40:Ch90	R1:R123	14,551,218	408,807

Graphical Representation of Attacks and Countermeasures



Individual Countermeasure Evaluation

Countermeasure Evaluation

SV = 430,106,901,440 units^3 → 1,000,000,000 €
AV($A_1 \cup A_2$) = 10,938,312units^3 → 25,431.61 € (ALE)
AIV = 3100 €

Counter-measure	Description	SC	EF	RM	ARC	RORI
C1.1	Behavioral detection	0.04	0.60	0.02	1,200€	-13.71%
C1.2	**Install Antivirus**	**0.30**	**0.70**	**0.21**	**1,000€**	**105.87%**
C1.3	Make all shares “read only”	0.30	0. 50	0.15	1,450€	51.97%
C2.1	**Install patches**	**0.25**	**0.70**	**0.18**	**1,250€**	**73.58%**
C2.2	**Block C&C domains**	**0.28**	**0.80**	**0.22**	**800€**	**125.46%**
C2.3	Create signatures IDS	0.04	0.75	0.03	2,000€	-24.26 %

Average = 53.19%

TELECOM SudParis

Combined Countermeasure Evaluation

Countermeasure	Description	SC	EF	RM	ARC	RORI
C1.2	Install Antivirus	0.30	0.70	0.21	1,000€	105.87%
C2.1	Install patches	0.25	0.70	0.18	1,250€	73.58%
C2.2	Block C&C domains	0.28	0.80	0.22	800€	125.46%

$RM(C_1 \cup C_2) = SC(C_1) \times EF(C_1) + SC(C_2) \times EF(C_2) - SC(C_1 \cap C_2) \times \min\{EF(C_1), EF(C_2)\}$

$ARC(C_1 \cup C_2) = ARC(C_1) + ARC(C_2)$

Countermeasure	SC(int)	EF(min)	RM	ARC	RORI
C1.2 & C2.1	0.10	0.70	0.31	2,250€	106.56%
C1.2 & C2.2	**0.00**	**0.70**	**0.43**	**1,800€**	**188.52%**
C2.1 & C2.2	0.00	0.70	0.40	2, 050€	157.23%
C1.2 & C2.1 & C2.2	0.09	0.70	0.55	3,050€	177.61%

Countermeasure Analysis

Additional Information

Counter - measure	Coverage (%)	Residual Risk (units[3])	Residual Risk (%)	Potential Collateral Damage (units[3])	Potential Collateral Damage (%)
C1.1	3.55%	10, 549,512	96.45%	818,100	67.79%
C1.2	30.06%	7, 649,712	69.94%	54,167,400	94.28%
C1.3	29.80%	7,678,197	70.20%	22,151,205	87.17%
C2.1	24.65%	8,241,660	75.35%	32,428,188	92.32%
C2.2	28.63%	7,806,312	71.37%	52,920,000	94.41%
C2.3	3.74%	10,529,505	96.26%	14,340,861	97.19%

Conclusion

- **I hope that I have shown you that counter-measures are an interesting subject**
  - Amongst others ☺
  - A natural extension to dynamic security monitoring
  - More to do than simply shut down

- **Many issues to solve**
  - In particular the opposition between availability and integrity/confidentiality

TELECOM SudParis