V-Research

Research & Development for Cybersecurity Engineering

The Etiology of Cybersecurity

The Science Club
knowledgezero@v-research.it

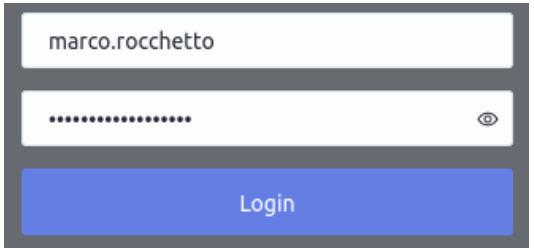
Dissemination level: Public
Confidentiality level: unencrypted
ECCN: NSR

https://v-research.it

Agenda

1. The problem in the Method
2. Cybersecurity Hypothesis
3. Risk Assessment Prototype

Necessary Cybersecurity Requirements

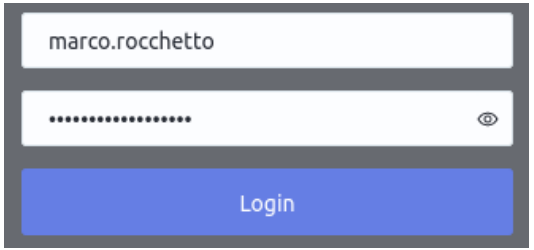


Jacob Nielsen (usability expert)
Usability suffers if users only get a row of bullets when they type their password.
Password Masking doesn't even increase security but cost you business due to login failures

Bruce Schneier (security expert)
[June 26, 2009] "I agree with this"
Epic flame-war
[July 3, 2009] "So was I wrong? Maybe. Okay, probably"

So, is this secure? More secure?

Necessary Cybersecurity Requirements



Jacob Nielsen (usability expert)
Usability suffers if users only get a row of bullets when they type their password.
Password Masking doesn't even increase security but cost you business due to login failures

Bruce Schneier (security expert)
[June 26, 2009] "I agree with this"
Epic flame-war
[July 3, 2009] "So was I wrong? Maybe. Okay, probably"

So, is this secure? More secure?

Is there a propriety P of a system S such that S is a secure system?

What is P? Confidentiality?
Confidentiality=security?
(it's tautological - it does what it does)
Security is something else

IEEE CYBER SECURITY

Unfalsifiability of security claims

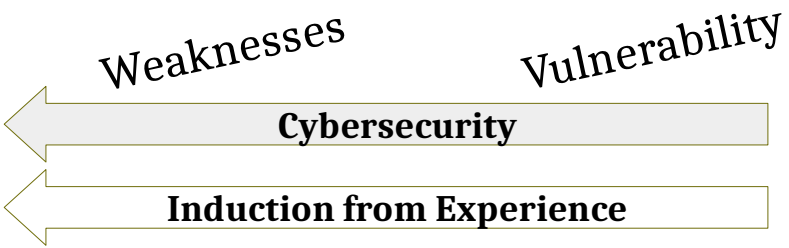
Cormac Herley[a,1]
[a]Microsoft Research, Redmond, WA 98052

There is an inherent asymmetry in computer security: Things can be declared insecure by observation, but not the reverse. There is no observation that allows us to declare an arbitrary system or technique secure. We show that this implies that claims of necessary

Theory

Reality

Errors



System under **attack**

Theory

Reality

Errors

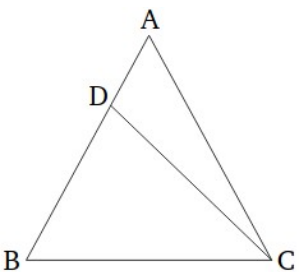
Weaknesses

Vulnerability

Cybersecurity

Induction from Experience

System under **attack**

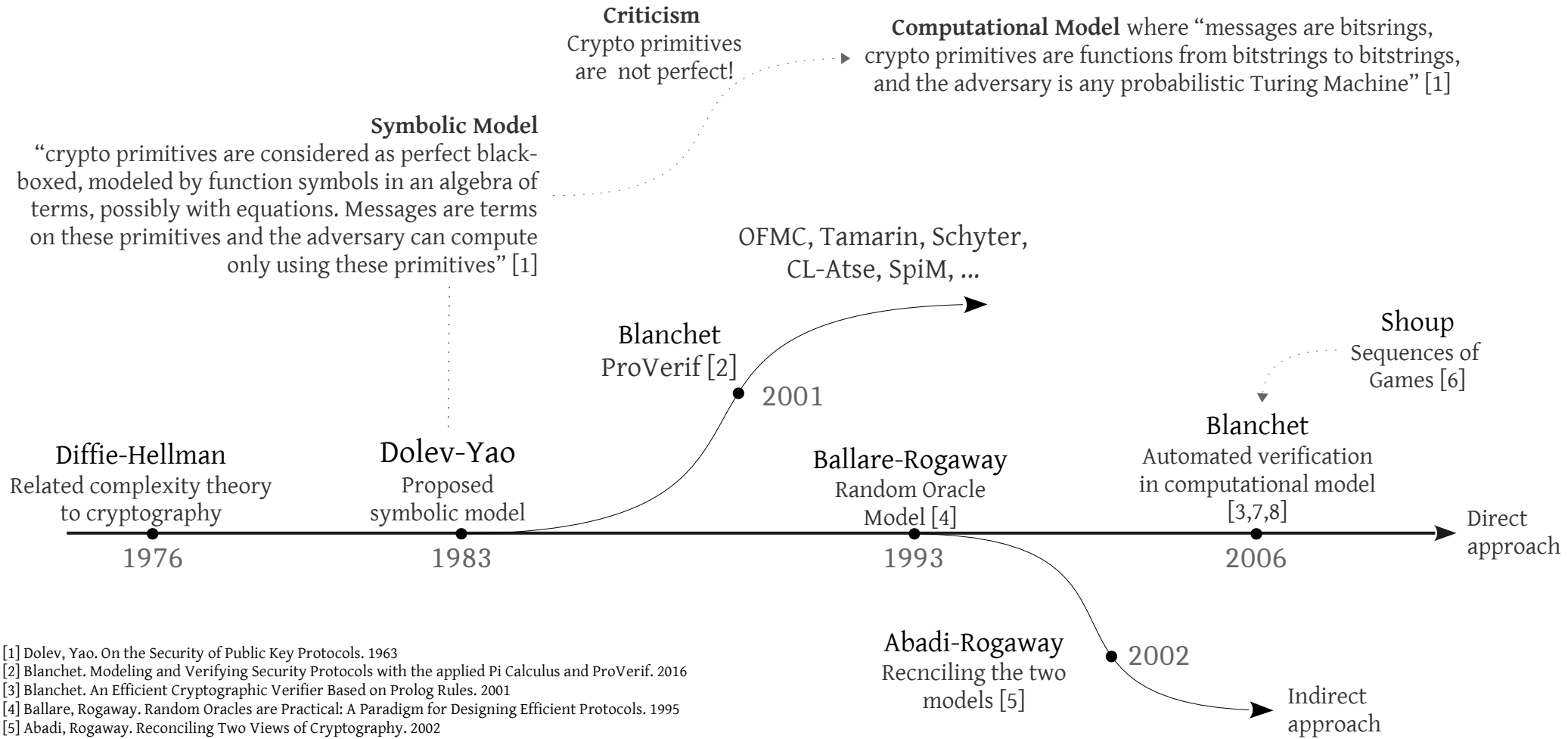


Euclid & **The scientific method**

Deduction/**Predictions**

If a triangle has two angles equal to one another
the sides subtending the equal angles
will also be equal to one another.

We Are Aware of Cybersecurity Theories



[1] Dolev, Yao. On the Security of Public Key Protocols. 1963
[2] Blanchet. Modeling and Verifying Security Protocols with the applied Pi Calculus and ProVerif. 2016
[3] Blanchet. An Efficient Cryptographic Verifier Based on Prolog Rules. 2001
[4] Ballare, Rogaway. Random Oracles are Practical: A Paradigm for Designing Efficient Protocols. 1995
[5] Abadi, Rogaway. Reconciling Two Views of Cryptography. 2002
[6] Shoup. Sequences of Games: a Tool for Taming Complexity in Security Proofs. 2004
[7] Blanchet. A Computationally Sound Mechanized Prover for Security Protocols. 2006
[8] Blanchet, Pointcheval. Automated Security Proofs with Sequences of Games. Advances in Cryptology. 2006

Agenda

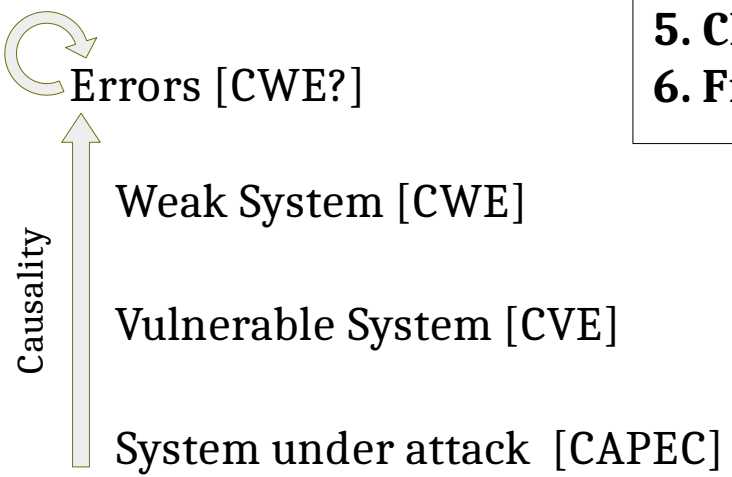
1. The problem in the Method
2. **Cybersecurity Hypothesis**
3. Risk Assessment Prototype

Cybersecurity Hypothesis

1. Claim: insecurity is generated by attacks
2. Claim: attacks are (caused) made possible by errors

3. Def: security is achieved when no attacks are possible
4. Hyp: a *theory on system errors* should predict insecurity

5. Challenge: how can we define a theory of errors?
6. First step: start from a theory of systems



What is a system?

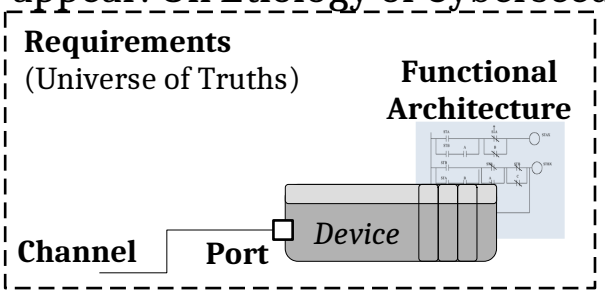
A belief revision system

Epistemology	Multi-Agent Systems		Cyber-Physical Systems
Knowledge	Fact	Fact	Architectural Requirements
Belief	Belief	Behavior	Functional Architecture
Information	Assertion	Assertion	Channels & Ports

[23] Jaakko Hintikka. "Knowledge and Belief: An Introduction to the Logic of the Two Notions". In: *Studia Logica* 16 (1962), pp. 119–122.

[24] Jakko Hintikka. "On proper (popper?) and improper uses of information in epistemology". In: *Theoria*. Wiley Online Library, 1993, pp. 158–165. URL: https://doi.org/10.1111/j.1755-2567.1993.tb00867.x.

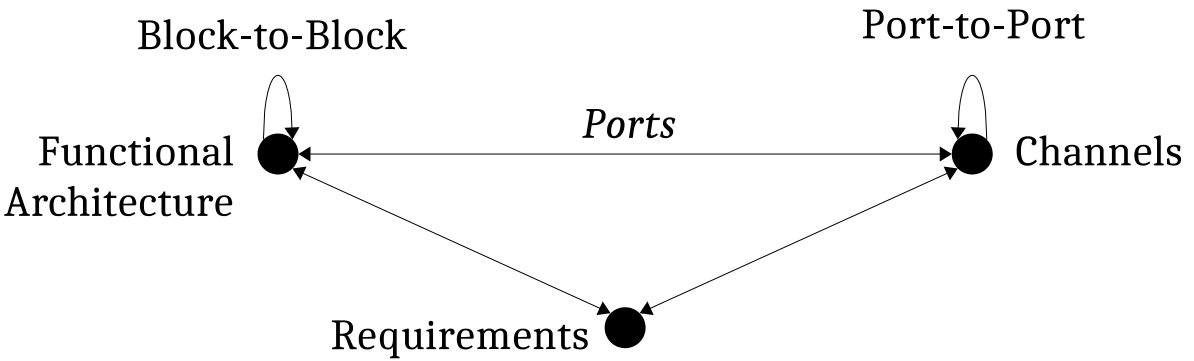
To appear: On Etiology of Cybersecurity



European Conference on Multi-Agent Systems
International Conference on Agreement Technologies
EUMAS 2016, AT 2016: Multi-Agent Systems and Agreement Technologies pp 261-276 | Cite as

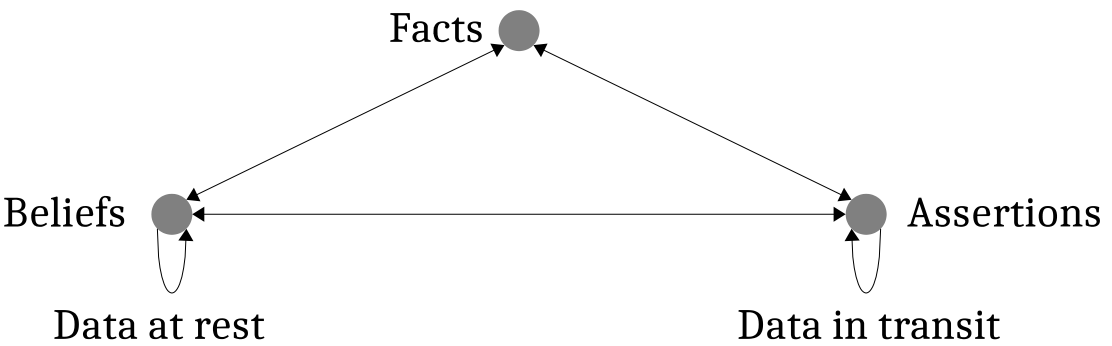
A Topological Categorization of Agents for the Definition of Attack States in Multi-agent Systems

ABF-Framework for System Design



Cyber-Physical Systems

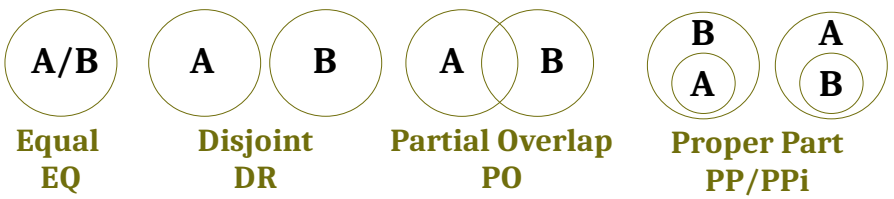
Multi-Agent Systems

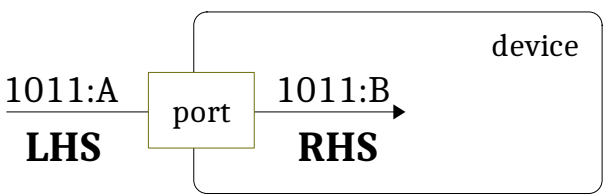


Cybersecurity Weakness Prediction (RIDI-Hypothesis)

There exist **3 categories of weaknesses**:

- B/F errors in *behaviors* (functional architecture)
- A/F errors in *communications* (channels)
- A/B errors in *translations* (ports)



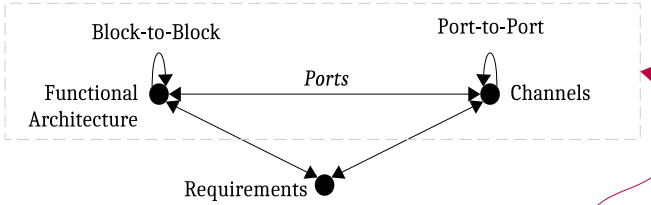


	RCC Calculus	LHS	RHS
nominal	EQ	x	$y = x$
replace	DR	x	$y \neq x$
insert	PP	x	$y = x \cdot x'$
delete	PPi	x	$y \subset x$
inject	PO	x	$y = x' \cdot y', x' \subset x, y' \neq x$

There are other (similar) weaknesses:
Selective drop
Selective drop+insert

From Errors to Architectural Weaknesses

quantity



This is general, an application to a specific requirement is provided afterwards

	RCC Calculus	R1	R2
nominal	EQ	x	$y = x$
replace	DR	x	$y \neq x$
insert	PP	x	$y = x \cdot x'$
delete	PPi	x	$y \subset x$
inject	PO	x	$y = x' \cdot y', x' \subset x, y' \neq x$

	Quantity: Data Flow between The input and output of: Channels(A,A); Ports(B,A); FunctionalBlocks(B,B)	**Quality**: Requirements (Facts) over Channel(A,F); Behavior(B,F)
EQ	Expected, Nominal	Expected, Nominal
DR	**drops** all the inputs and **inserts** new malicious data	the component never performs/carries the expected behavior/information
PP	selectively **drops** inputs	part of the expected outputs are not generated in response to the correct inputs
PPi	forwards all the inputs but **crafts** and **inserts** new malicious data	the components correctly performs/carries the expected behavior/information when the correct inputs are provided but is subject to input injections
PO	selectively **drops** inputs and **inserts** new data	Byzantine behavior - occasionally outputs the expected output given the correct inputs. Not all the inputs are handled properly, nor all the expected outputs are always generated when correct inputs are given

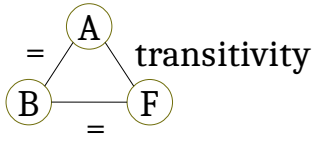
Cybersecurity Quantitative Evaluation

Cybersecurity = 1 – (many - some)

The **secure** configuration where all the components of the system have no errors

All the **insecure** configurations where an error occurs in (at least) one device

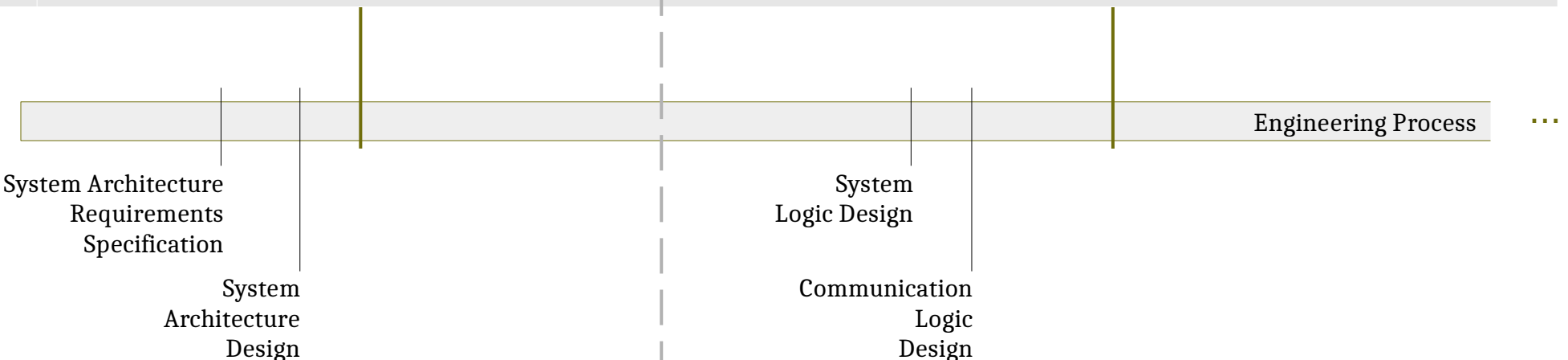
Mathematically, not all the errors may occur simultaneously



This allows us to precisely measure security risks
We have a metric for security

Cybersecurity Abstract Attacks – *Not-so-easy* Next Steps

	Quantity: Data Flow between The input and output of: Channels(A,A); Ports(B,A); FunctionalBlocks(B,B)	**Quality**: Requirements (R) over Channel(A,R); Behavior(B,R)
EQ	Expected, Nominal	Expected, Nominal
DR	**drops** all the inputs and **inserts** new malicious data	the component never performs/carries the expected behavior/information
PP	selectively **drops** inputs	part of the expected outputs are not generated in response to the correct inputs
PPi	forwards all the inputs but **crafts** and **inserts** new malicious data	the components correctly performs/carries the expected behavior/information when the correct inputs are provided but is subject to input injections
PO	selectively **drops** inputs and **inserts** new data	Byzantine behavior - occasionally outputs the expected output given the correct inputs. Not all the inputs are handled properly, nor all the expected outputs are always generated when correct inputs are given



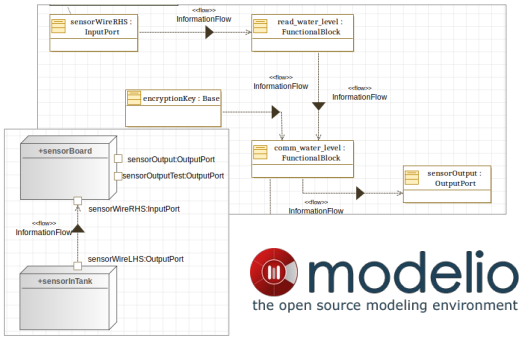
V-Reseʌrch

Agenda

1. The problem in the Method
2. Cybersecurity Hypothesis
3. Risk Assessment Prototype

Automated Cybersecurity Risk Assessment

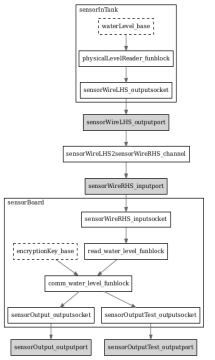
1. System Engineering

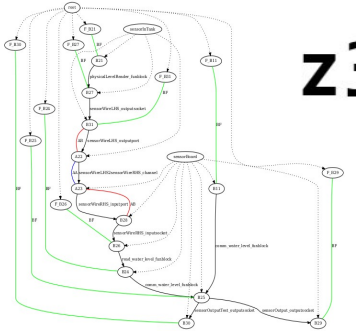


modelio
the open source modeling environment

GitHub
git
AGPL v3
Free Software
Free as in Freedom

2. Automated Threat Scenario Generation & Reasoning





z3 Microsoft Research

3. Automated Risk Estimation & Mitigation Suggestions

	B	C	D	E	F
	Agent	**Component**	**Comp. Type**	**Weakness**	**Status**
	sensorBoard	sensorWireRHS	inputport	selectively drops inputs and inserts new malicious data	open
	root	sensorWireLHS2sensorWireRHS	channel	selectively drops inputs and inserts new malicious data	open
	sensorInTank	sensorWireLHS	outputport	selectively drops inputs and inserts new malicious data	open
	sensorInTank			the component has a Byzantine behavior where occasionally outputs the expected output given the correct inputs. Not all the inputs are handled properly, nor all the ways generated given.	open

52	**RISK**	16777216
53	The total risk is the total number of configurations of the system	

4. on-the-fly Risk Reduction Based on Mitigation

V-Research

V-Research – Risk Assessment Prototype

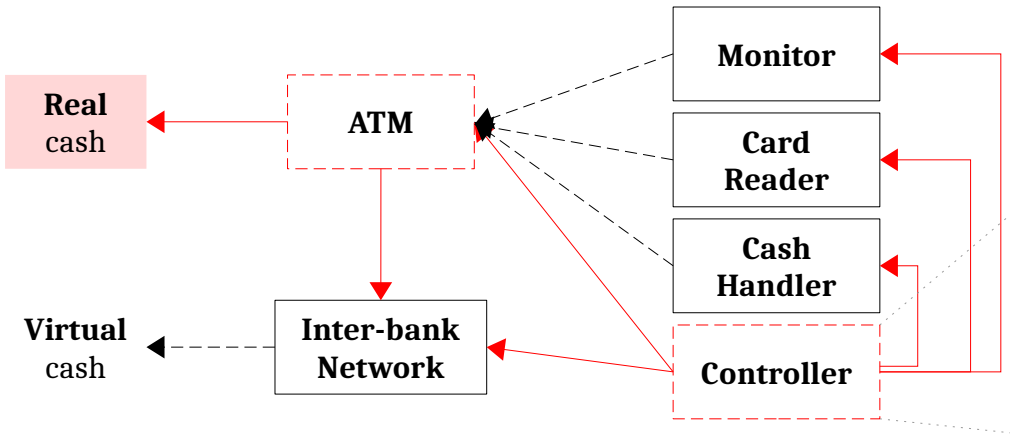
Complete Prediction of Cybersecurity Flaws
Without Databases of Known Attacks!

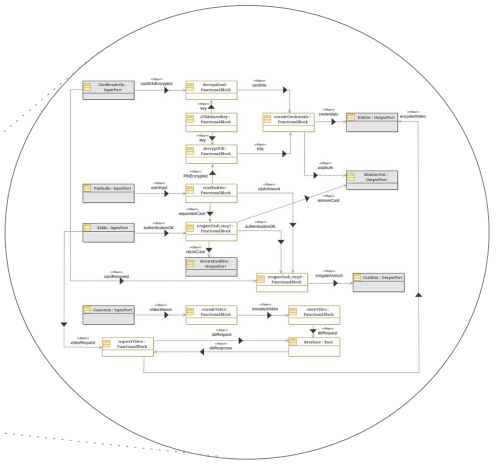
Agent	Component	Component Type	Potential Architectural Weakness	Weakness ID	Weight	Status	Assignee
ATMcontroller	ATMsharedkey	Functional Block	the component has a Byzantine behavior where occasionally outputs the expected output given the correct inputs. Not all the inputs are handled properly, nor all the expected outputs are always generated when correct inputs are given.	W001	1	mitigated	*Mario Rossi*
			part of the expected outputs are not generated in response to the correct inputs	W002	1	mitigated	*Mario Rossi*
			the components correctly performs the expected behavior when the correct inputs are provided but is subject to input injections	W003	1	open	
			the component never performs the expected behavior	W004	1	open	
	CameraIn	Input Port	alters incoming messages producing malicious requests for the connected input socket or functional block	W005	4	open	
			appends new requests to the incoming messages	W006	4	open	
			selectively drops some of the incoming messages	W007	4	open	
			drops all the incoming messages and substitute them with new malicious ones	W008	4	open	
		Input Socket	the component correctly translates some of the incoming requests to the functional architecture. Not all the incoming requests are properly translated, nor all the expected requests are always produced.	W009	1	open	
			part of the generated requests are not generated in response to the correct inputs	W010	1	open	
			the components correctly generate the incoming requests when the correct inputs are	W011	1	open	

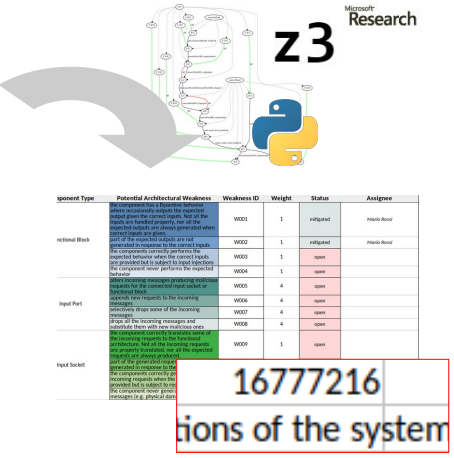
RISK	16777216
The total risk is the total number of insecure configurations of the system	

V-Research: Security By Design

Architecture → Risk Assessment







Asset (Bank) — System (stakeholders)

Physical Architecture — Logic (sub-systems)

Phase 1
Asset Diagram

Phase 2
Architecture

Phase 3
Automated Risk Assessment

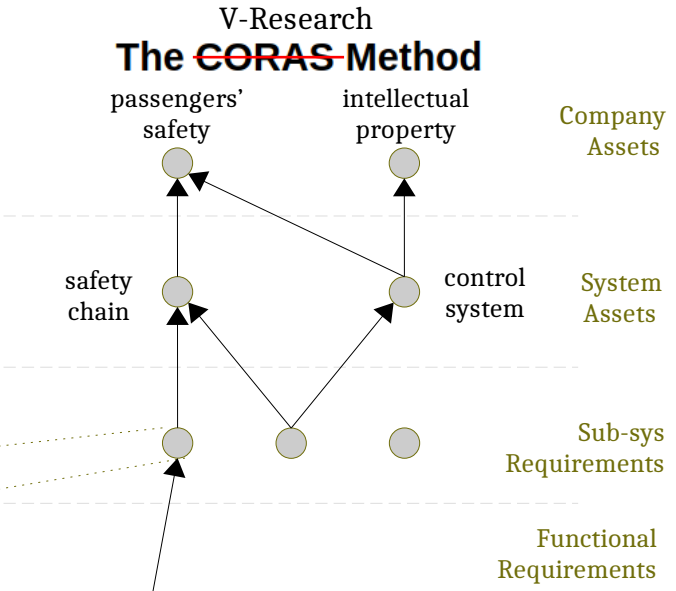
V-Research

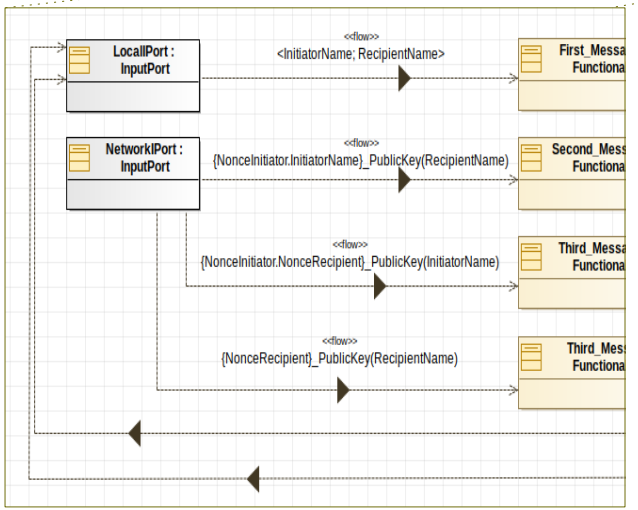
THΛNK YOU

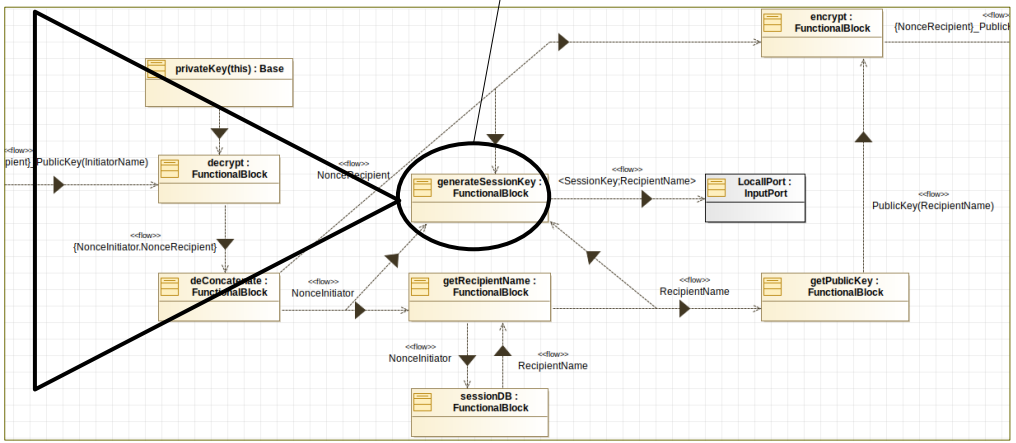
Q&Λ

Cybersecurity Risk Assessment – *Easy* Next Steps

1) Asset Diagrams and Cone of Influence (Impact)
2) Language Standard Form (SysML-Modelio, SysML-IBM Rational, …)
3) Library (Primitive) Implementation
4) Alignment to Cybersecurity Domain-specific Standards and Safety Standards
5) Software Engineering & Licensing



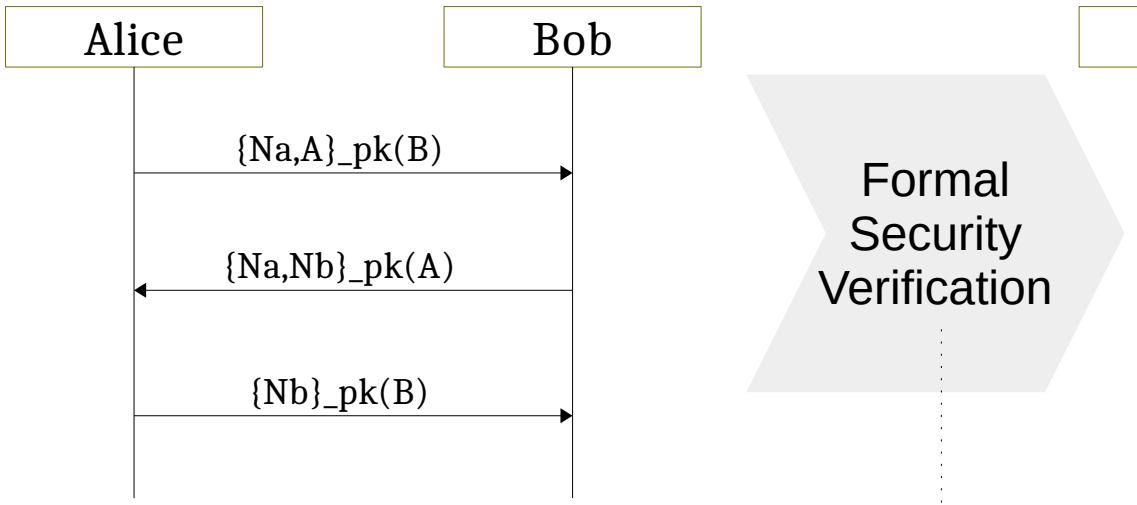




V-Research

Current Cybersecurity SotA on Protocol Logic

Incomplete Protocol Model → **Incomplete** Attacker Model → Very **Interesting** Attacks



Formal Security Verification

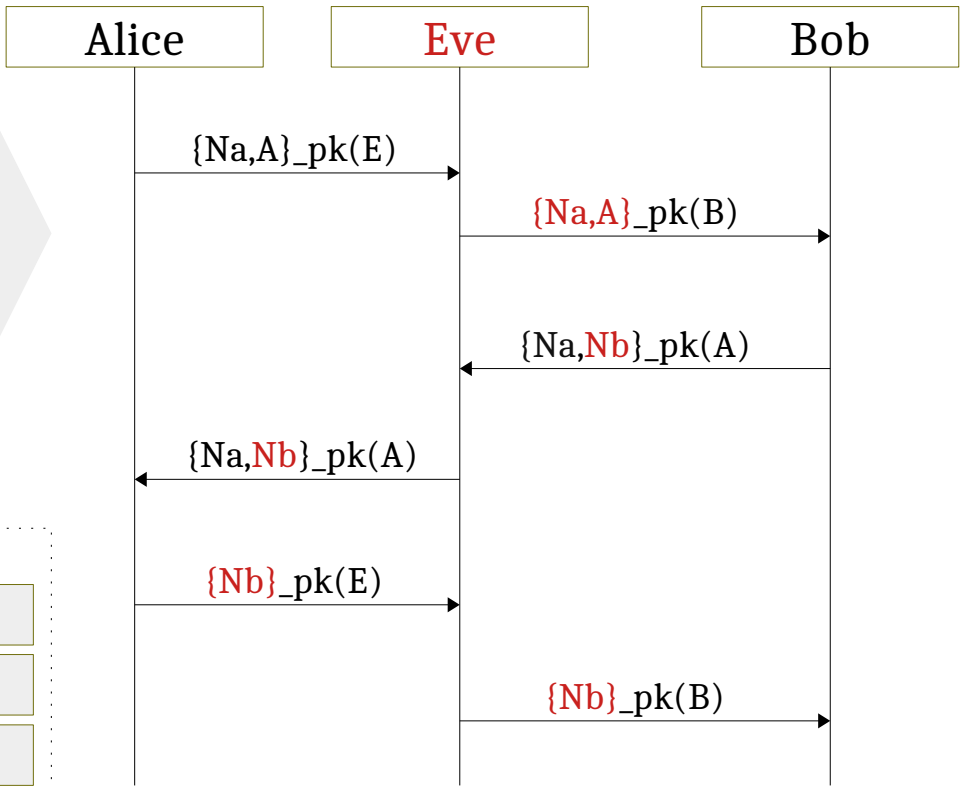
$$\frac{M_1 \in M}{M_1 \in DY}\ G_{\text{axiom}} \qquad \frac{M_1 \in DY \quad M_2 \in DY}{[M_1, M_2] \in DY}\ G_{\text{pair}} \qquad \frac{M_1 \in DY \quad M_2 \in DY}{\{M_1\}_{M_2} \in DY}\ G_{\text{crypt}}$$

$$\frac{M_1 \in DY \quad M_2 \in DY}{\{|M_1|\}_{M_2} \in DY}\ G_{\text{scrypt}} \qquad \frac{[M_1, M_2] \in DY}{M_i \in DY}\ A_{\text{pair}_i} \qquad \frac{\{|M_1|\}_{M_2} \in DY \quad M_2 \in DY}{M_1 \in DY}\ A_{\text{scrypt}}$$

$$\frac{\{M_1\}_{M_2} \in DY \quad inv(M_2) \in DY}{M_1 \in DY}\ A_{\text{crypt}} \qquad \frac{\{M_1\}_{inv(M_2)} \in DY \quad M_2 \in DY}{M_1 \in DY}\ A^{-1}_{\text{crypt}}$$

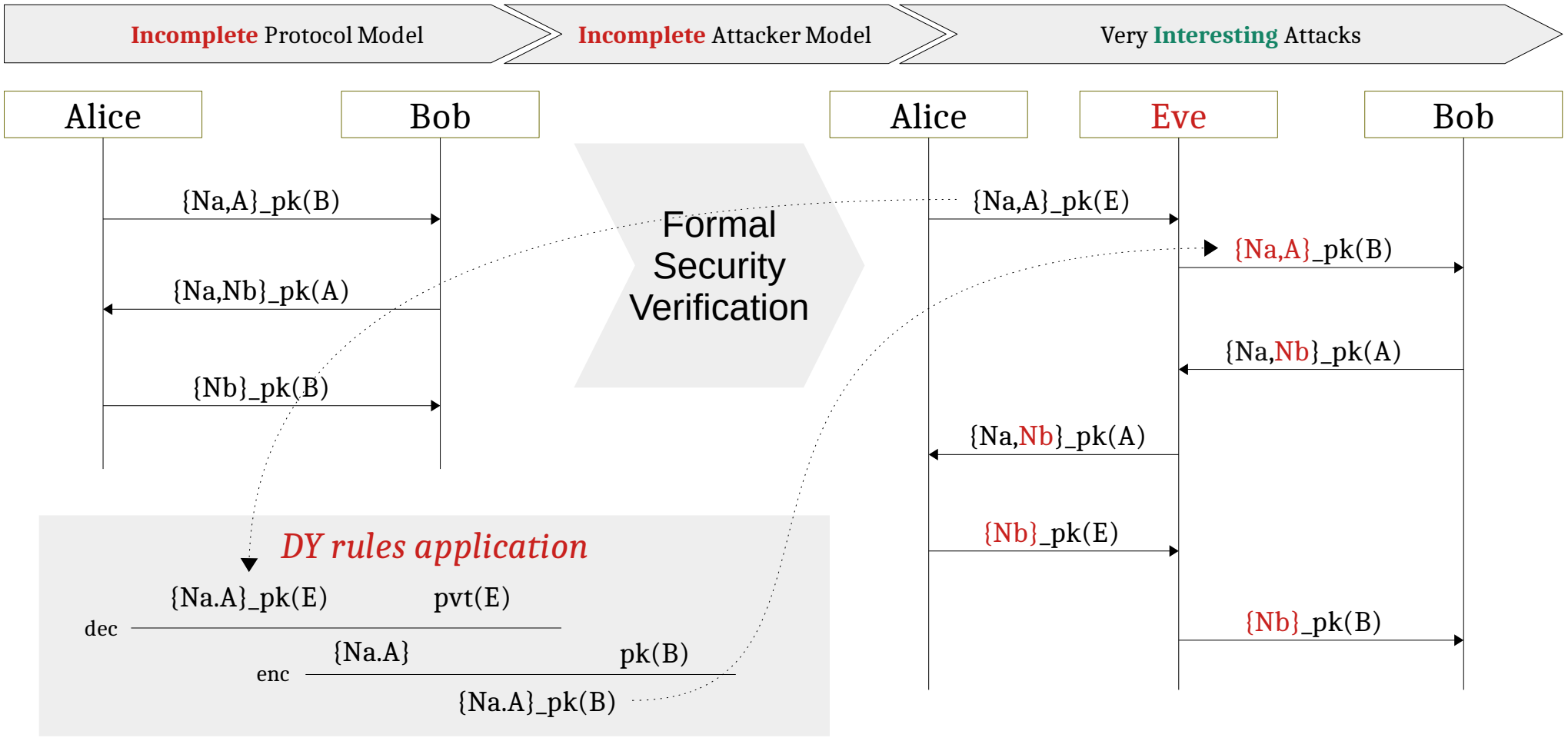
Fig. 2: The system of rules of the Dolev-Yao attacker

- Nonce freshness
- Message Order
- Key Leakage



V-Research

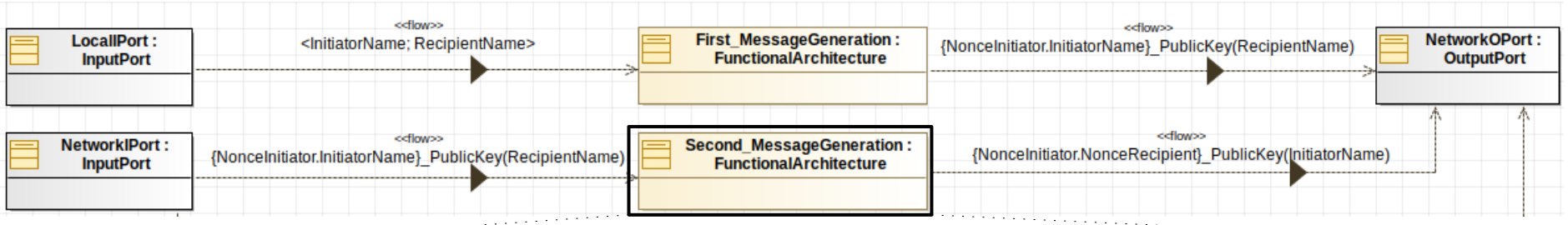
Current Cybersecurity SotA on Protocol Logic

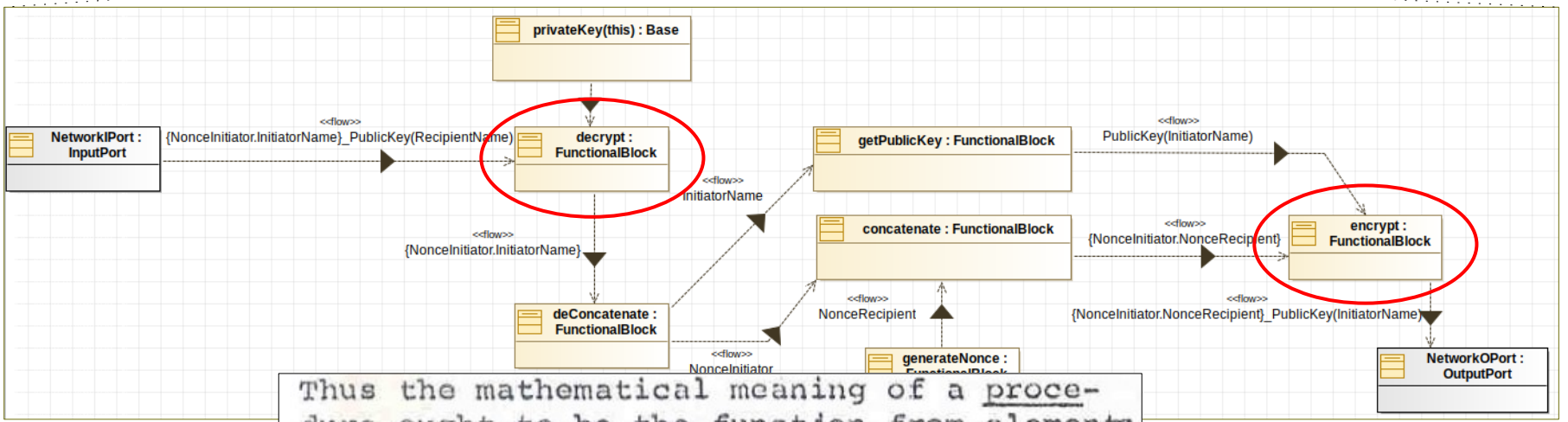


V-Research

What if... we listen to Dana Scott?

UML Model of the Function(s)/-al architecture → NO Attacker Model Model Checking (SPIN) → Very Interesting Attacks?





Thus the mathematical meaning of a procedure ought to be the function from elements of the data type of the input variables to elements of the data type of the output.

V-Research

V-Research Cybersecurity Theory

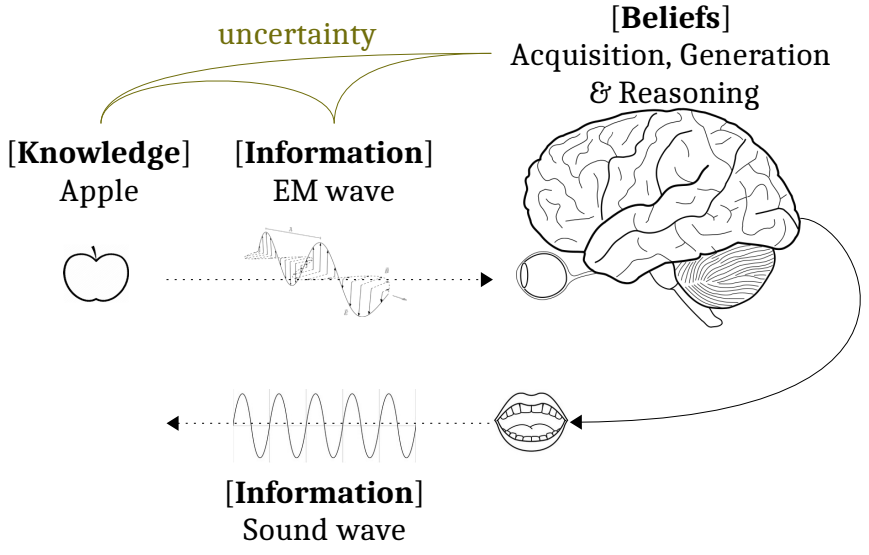
We developed our theory from Jaakko Hintikka's works, mapping epistemological concepts to system engineering

Epistemology

Set of Truths – **Knowledge**

Poorly Justified Statements – **Beliefs** — Error?

Transfer of Beliefs – **Information**



Multi-Agent Systems

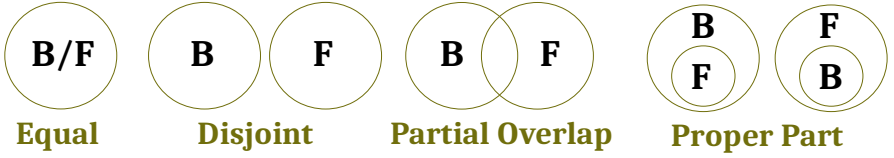
Facts – Ground Truths/Environment

Behaviors – Agent's thoughts

Assertions – Agent's communication

European Conference on Multi-Agent Systems
International Conference on Agreement Technologies
EUMAS 2016, AT 2016: Multi-Agent Systems and Agreement Technologies pp 261-276 | Cite as

A Topological Categorization of Agents for the Definition of Attack States in Multi-agent Systems



Given a calculus (RCC5) over a topology

- B/F errors in behaviors
- A/F errors in assertions
- A/B errors in translations