We hit "glass ceiling(s)" years ago! Blackhats are winning unless we change!

Dr. Ulrich Lang, CEO
ulrich-lp@objectsecurity.com
650-515-3391
ObjectSecurity LLC

Disclaimer

The views and opinions expressed during this conference are those of the speaker and do not necessarily reflect the views and opinions held by the ObjectSecurity LLC company, the Information Systems Security Association (ISSA), the Silicon Valley ISSA, the San Francisco ISSA or the San Francisco Bay Area InfraGard Members Alliance (IMA). Neither ISSA, InfraGard, nor any of its chapters warrants the accuracy, timeliness or completeness of the information presented. Nothing in this conference should be construed as professional or legal advice or as creating a professional-customer or attorney-client relationship. If professional, legal, or other expert assistance is required, the services of a competent professional should be sought.

Clarifications

- "Glass ceiling(s)" (in this talk): Invisible difficult barriers some stakeholders put in place that prevent others from progressing
- Controversial! Don't like it? – that's ok!
  - *Disclaimer: Much of this is a high-level discussion of the speaker's personal views, not a technical presentation with immediate "take-home" tools*

Presentation Outline

- Problem: Cyber security & privacy progress is too slow
- Case study: ObjectSecurity OpenPMF
- Who's "fault" is it?
- What "solutions" do we have?

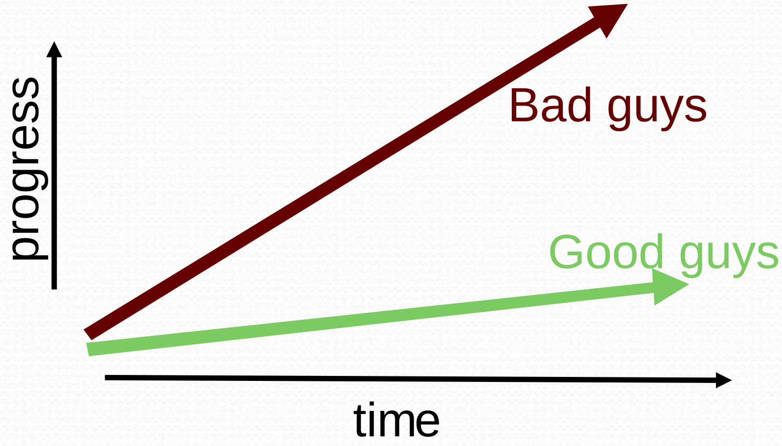
Dr. Ulrich Lang
CEO & Co-founder, ObjectSecurity
InfoSec PhD (Cambridge), & Master's (RHUL London)
CSA SV chapter board member, blogger, 5 patents,
>150 publications/presentations, book author, expert witness, …

Problem

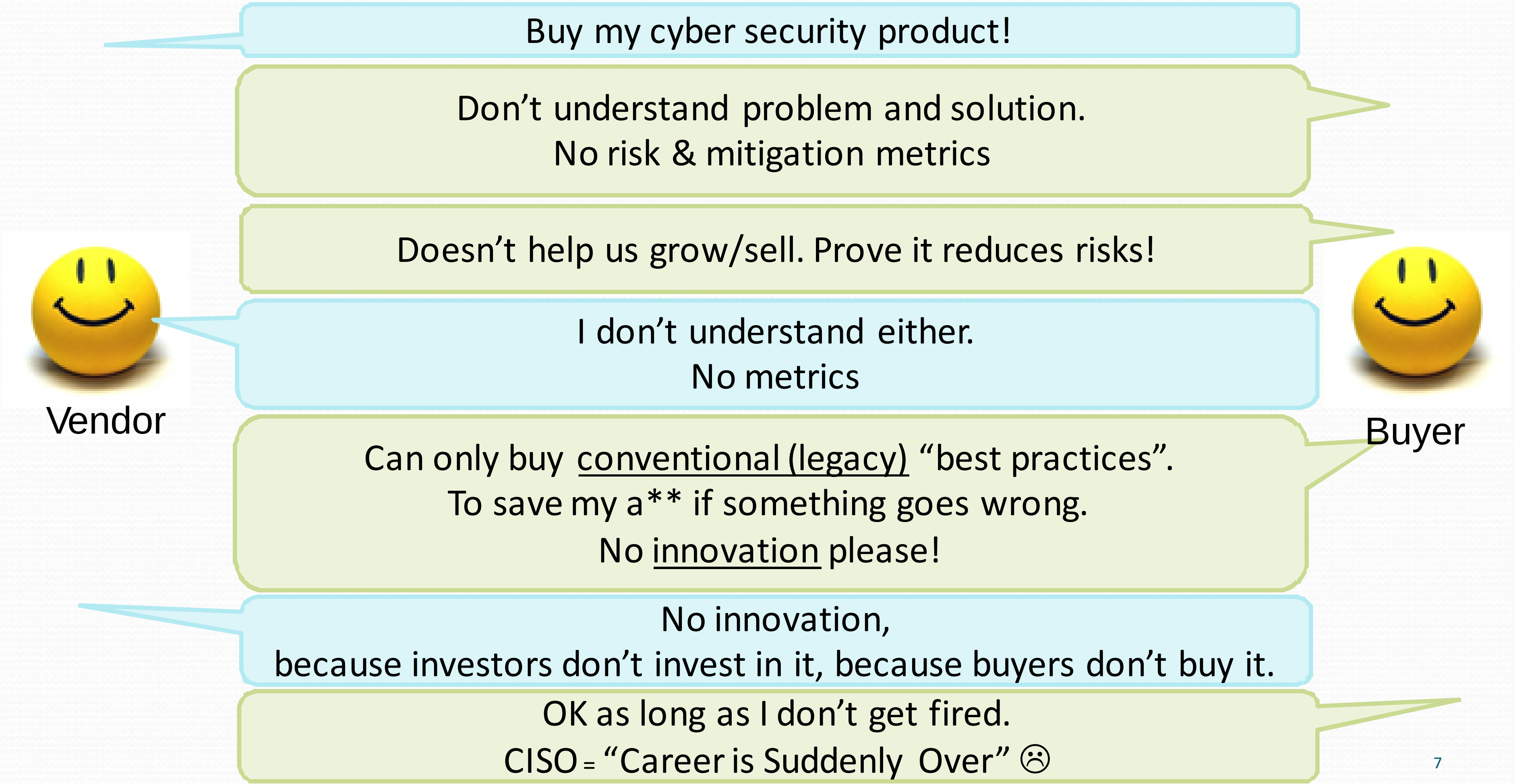
Cyber security & privacy progress is too slow
to keep up with the attackers

Let’s define the problem

- cyber security ecosystem is progressing too slowly
- few game-changers find adoption:
  - e.g. ABAC?, micro kernels?, privacy avatars? “good guys”: severe constraints (economic and otherwise)
- “bad guys”: better working ecosystem, and smaller problem to solve)
- how to break through the vicious cycle?



A cynic’s guide to cyber security selling (excerpt)



Buy my cyber security product!

Don’t understand problem and solution.
No risk & mitigation metrics

Doesn’t help us grow/sell. Prove it reduces risks!

Vendor

I don’t understand either.
No metrics

Buyer

Can only buy conventional (legacy) “best practices”.
To save my a** if something goes wrong.
No innovation please!

No innovation,
because investors don’t invest in it, because buyers don’t buy it.

OK as long as I don’t get fired.
CISO = “Career is Suddenly Over” ☹

“Market failure” defined

- definition:
  - inefficient allocation of goods/services
  - based on pure self-interest
  - can be improved from a societal point of view
- causes:
  - time-inconsistent preferences, information asymmetries, non-competitive markets (market power), principal–agent problems, externalities, or public goods
- Interventions:
  - self-regulatory organizations, governments or supra-national institutions

(roughly based on w ikipedia definition)

Market failure: cyber security

- Intractable: can’t quantify the problem or the solution
  - problems: attack vectors? risk/impact metrics?
  - solutions: reliable success metrics?
- Incomprehensible:
  - problems: do buyers understand? Do they want to know?
  - solutions: Can vendors make buyers understand the solutions? Do vendors know 100%?
- Information asymmetry seller-buyer

Market failure: cyber security

- Hard-to-quantify value: “negative sell”, unclear effectiveness
- Lack of accountability: product disclaimers etc.
- Externalities: Buyer often not the affected stakeholder
- Fewgood damage metrics:
  - e.g. cost of data breach from Verizon and Ponemon
  - Do you still shop at Target, Home Depot etc.?
- Security trade-off: Security often slows down systems, decreases usability, etc.

Market failure: cyber security

- Attacker-defender asymmetry: Attacker only needs to win once, defender every time
- Doomsday narrative & industry direction:
  - Former Plan B (detection/remediation of sh** already going down) now often Plan A (i.e. first line of defense) ☹
    - “Prevention doesn’t work”, “remediation is the new prevention”, “continuous monitoring is the best defense”, “response and recovery”…
  - Compliance instead of security: paper-shuffling with % cooked up

Stopping here, but there is more…

Attackers

- Profit-driven cyber criminals
- Nation-states
- Malicious or accidental insiders
- Hacktivists
- …

Who’s “fault” is it?

Which stakeholders do what, and what is the effect?

the user’s fault?

- often the damaged stakeholder
- often not the buyer
- will usually not “vote with their feet”
  - can’t determine security quality, security need, vendor lock-in

The buyer’s fault?

- often don’t care
  - because unclear ROI, benefits, metrics, no interest/time
- often do minimum required to meet compliance
  - because of (perceived) unclear ROI
- often cannot adopt innovative security due to constraints
  - technical, financial, organizational, operational, cultural, educational, risk appetite (ironically!), personal risk

The vendor's fault?

- cannot commercialize disruptive cybersecurity -> won't sell
- incumbent security vendors/primes/integrators can reduce/defer their own cost and risk by blocking innovation
- changing buyer mindset to embrace something new takes a long time (sometimes 10-30 years)
- hi-tech entrepreneurs usually don't care much about security unless it's needed to make the business run
  - business failure risk much higher than security failure risk
  - time-to-market, cost savings, user experience etc. all count more
  - if users don't care/know, why invest in security?

The investor’s fault?

- business of making money, not to change/improve the world
  - If dogsh** sells now, invest in dogsh** ☺
- won’t invest in true security innovation because it won’t sell quickly:
  - educating market is expensive, time-consuming, risky, against “herd”
- to minimize risks:
  - only invest in minor, incremental improvement to reduce risk and time-to-exit (“timing is everything”)
  - only invest in “tried & tested” teams and technologies

The academic researcher's fault?

- In theory: fundamental cybersecurity research to come up with new solutions (15-30 year timeframe to mainstream)
- In practice, most of the research won't change the world
  - Nobody can predict IT that far out
  - Irreconcilable: teaching vs. research
  - Often don't know anything about the real world
  - Most researchers' own goals more important (e.g. publishing)

The government's fault?

- Government intervention #1 measure to fix market failures
- Gov. used to take the lead in IT and cybersecurity innovation
  - Now "looking to industry", but limited funds, inefficiencies, earmarks, sequester, bureaucracy, …
- However: Our physical security (military, police etc.) is run by government for good reasons. Why is cybersecurity different?
- Mandate cyber security through regulation (e.g. HIPAA)
- Unfortunately often no "teeth":
  - take calculated risks; non-mandatory; self-regulation etc.

The educator’s fault?

- Should educate the public about security and privacy
  - Societal understanding would maybe create a market
  - Users would maybe “vote with their feet” if they understood risks and solutions
  - Should be taught in school and at university
- Reality (see “Users” earlier):
  - Most people don’t care, don’t understand, falsely trust the provider/vendor

Stopping here, but there is more…

So whose fault is it?

- Everyone's!
- In particular:
  - Customers: A "free market" (if it worked) is ultimately driven by customers.
  - Government: Intervene to adjust market failures, esp. externalities, antitrust etc.
  - Vendors & Investors: Stuck in the middle

Case Study: Cybersecurity innovation from the “trenches”

Theoretical discussion? Or are these problems real?

Or is the lack of progress the innovators’ fault?

ObjectSecurity® OpenPMF™

Model-Driven Security Policy Automation

Founded July 2000…model-driven security invention since 2003…now it's 2015!!!

The Security Policy Automation Experts

information security specialists: innovative technologies + consulting, R&D

CUSTOMERS

ITS, ATC, Defense & Aerospace, Manufacturing, ICT, Smart Cities

QinetiQ | UK MoD

BAA | UK TSB | Artechhouse

Cyber Security KTN | Intel | ESG | SAP

Royal Bank of Scotland | Twinsoft/HP | BMVIT

European Commission | Deutsche Telekom

European Space Agency | Lufthansa Systems

Eurocontrol | Hornbach | UL VS

US Naval Research Laboratory

Promia (US Navy)

Agilent

Smartronix

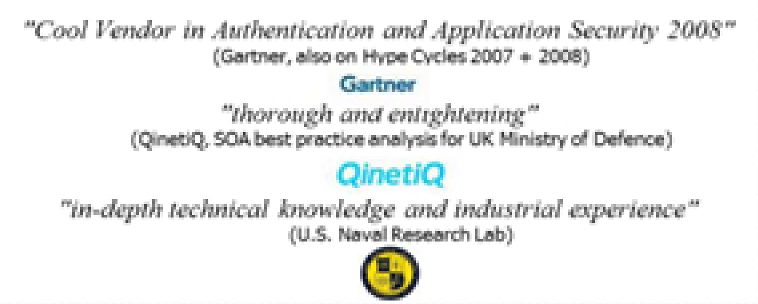
IBM

CHI

RTI (US Navy+ Air Force)

FutureTek (Boeing)

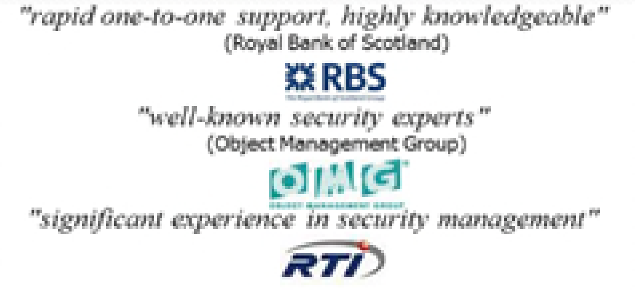
General Electric



"Cool Vendor in Authentication and Application Security 2008"
(Gartner, also on Hype Cycles 2007 + 2008)
Gartner

"thorough and enlightening"
(QinetiQ, SOA best practice analysis for UK Ministry of Defence)
QinetiQ

"in-depth technical knowledge and industrial experience"
(U.S. Naval Research Lab)



"rapid one-to-one support, highly knowledgeable"
(Royal Bank of Scotland)
RBS

"well-known security experts"
(Object Management Group)
OMG

"significant experience in security management"
RTI

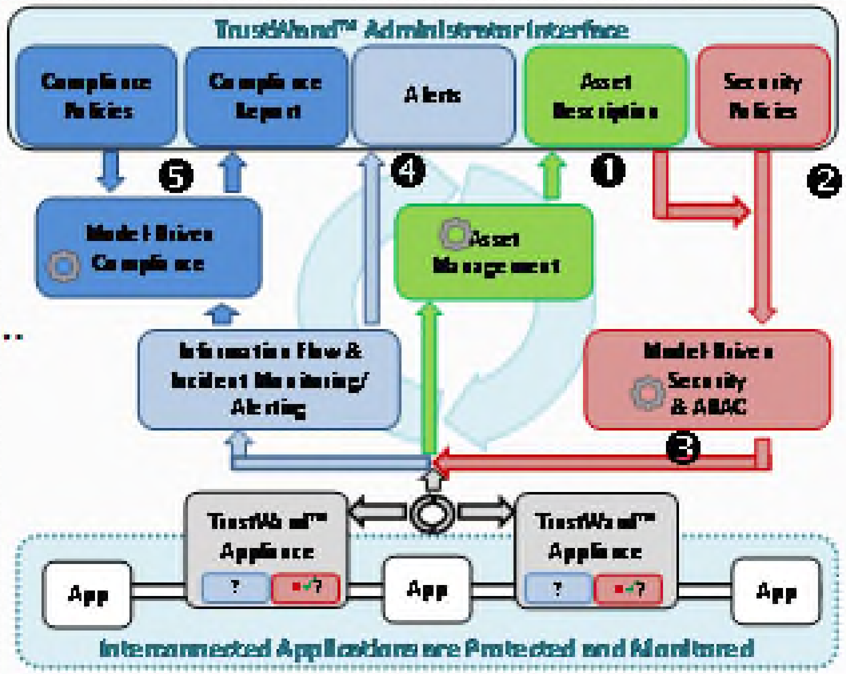
Glass ceiling - white hats are wasting time!!!

- 2000-2014 University R&D since 1997, startup since 2000…now 2015!
  - Industry "group-think" was blacklisting, compliance-based "security", monitoring/remediation as "Plan A"
    - Preventive white-listing, with end-point agents, and "doing policy right" not "group-think"
  - Market tanked at critical times:
    - Dot-com burst prevented high-growth at the beginning
    - Great recession just after brief high-visibility phase (e.g. 2008 Gartner "Cool Vendor")
  - Large vendors/integrators ignored/blocked this innovation
  - Customers often did not care (more concrete interest since about 2012)
  - "Staleness" (VC speak)

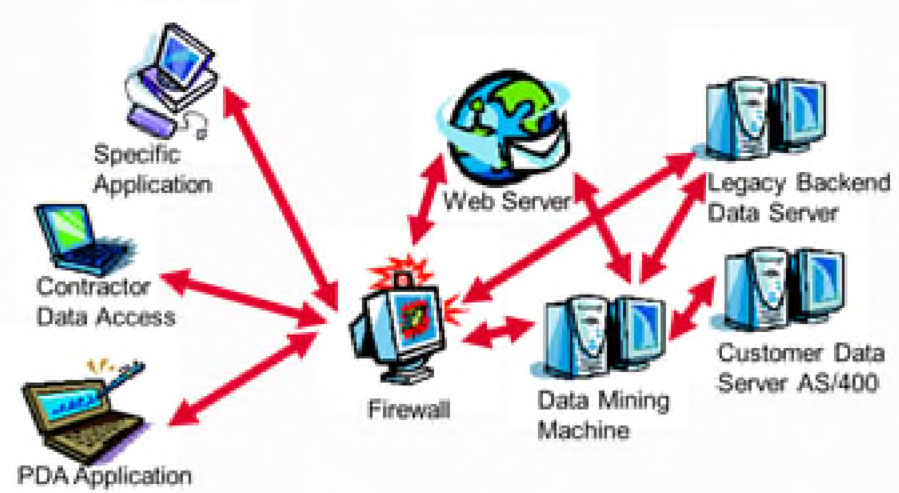
Glass ceiling - white hats are wasting time!!!

- 2014/2015: Strong IT investment market,
  - closing joint venture deal with partner Promia for TrustWand (incl. OpenPMF).
  - Investment for: Incremental improvement over current state, over a decade later…

University R&D since 1997,
startup since 2000…now 2015!



2000 …Middleware Security

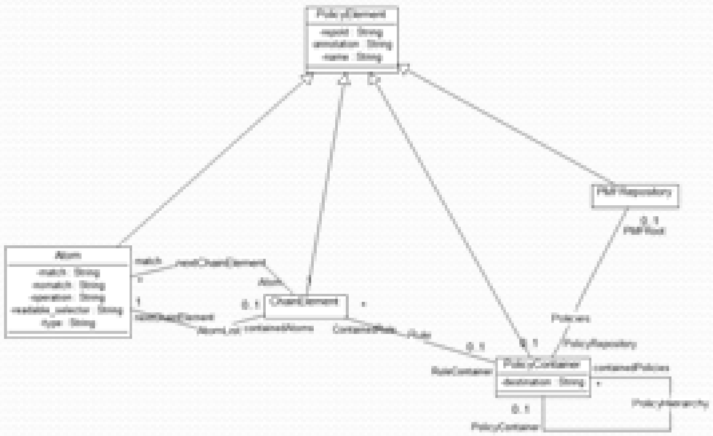


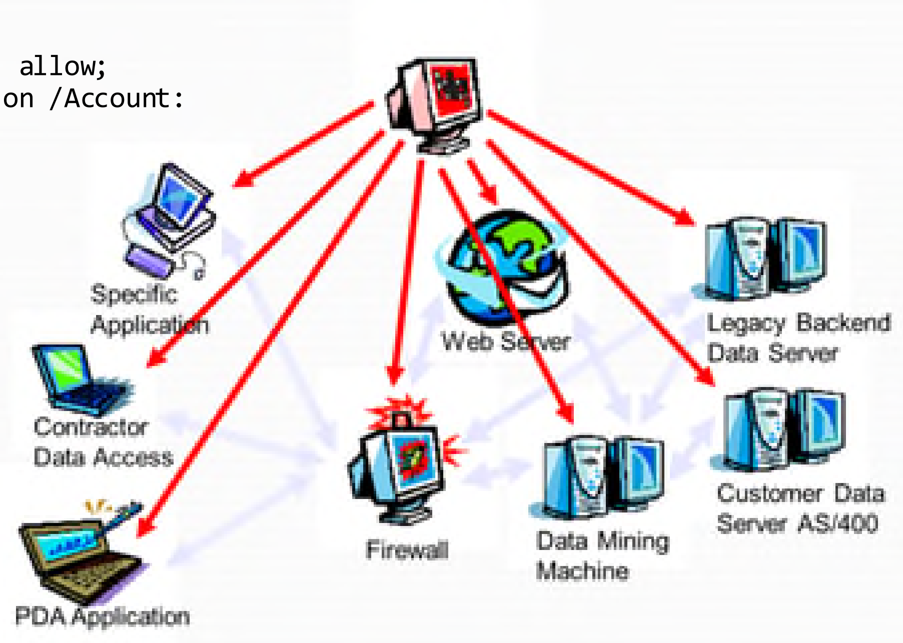
Implementing policies too difficult:

- Too many rules (whitelisting) in too many places
- Too many dynamic changes (agility)
- Policy support not expressive enough
- No assurance
- …

2002 …OpenPMF v1 (ABAC)

```
policy /OS {
   /OS/alice invokes {create, open} on /OS/Bank: allow;
   /OS/alice speaksfor /OS/bob invokes withdraw on /Account:
{allow, log}, {deny,log};
   * in /OS/staff uses /OS/server: allow
  };
```

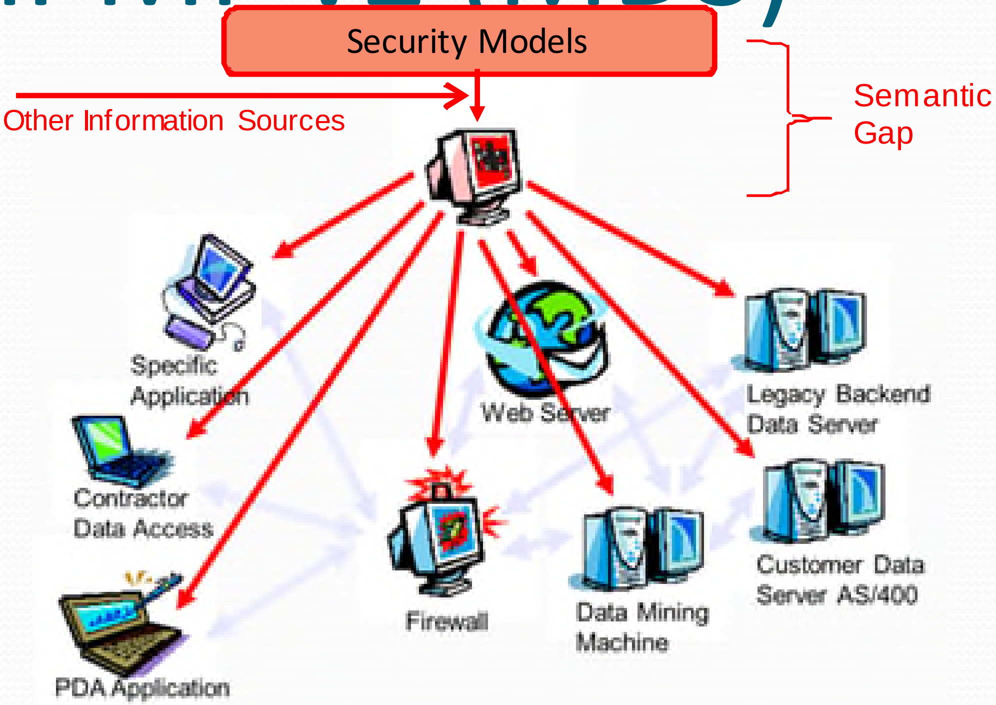




<u>Implementing policies too difficult:</u>

- Still too many rules, now in one place
- Too many dynamic changes (agility)
- Policy support not expressive enough
- Little assurance
- …

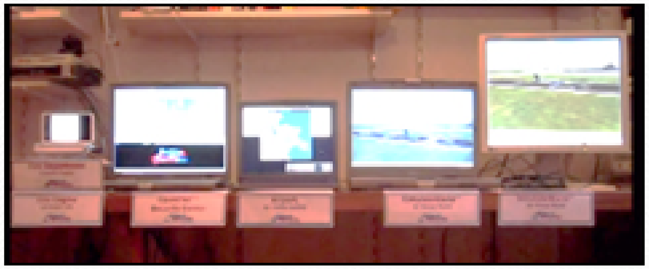
2004 …OpenPMF v2 (MDS)



Security Models

Other Information Sources

Semantic Gap

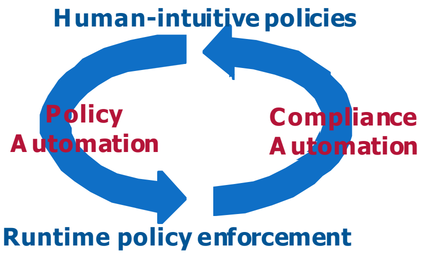


2007 started patenting, 2014 first patent granted, 2015 2nd patent. Now 8 years after filing 15 years after founding.

OpenPMF

Model-Driven Security:

- ✓ cheaper
- ✓ more secure
- ✓ faster accreditation/compliance
- ✓ for agile, complex IT landscapes
- ✓ standards



Human-intuitive policies

Policy Automation

Compliance Automation

Runtime policy enforcement

Challenges are growing & converging!

- IT environment
  - agile, complex, interconnected “System of Systems”
- Policies
  - numerous, complex, meaningful/feature-rich (e.g. privacy), fine-grained, contextual/dynamic
- Status quo fails
  - blacklisting; anomaly/behavior/incident-based; manual policy implementation…
- Need better policy tools
  - meaningful, preventive (whitelisting), manageable, supports IT agility, information flow based, repeatable/traceable/verifiable

Business problem has existed for >15 years, but the IT industry today still acts as if it is a new/future problem

Model-Driven Security

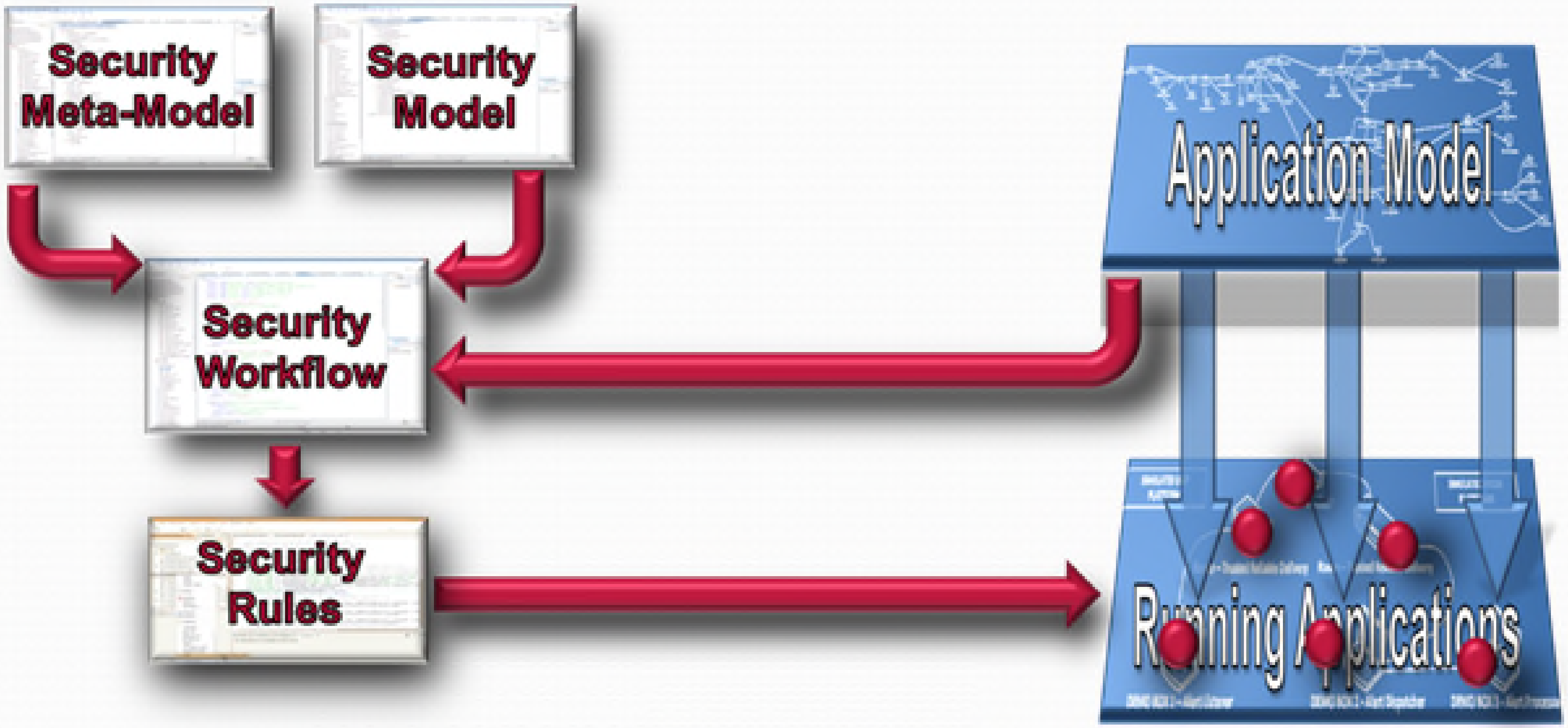
University research since late 90's, our invention since ca. 2003…now it's 2015!

- Information flow based SoS security (users & devices)
  - IoT/M2M often has system description & well-defined M2M interactions
- Access policies
  - Whitelisting; meaningful access policies; support IT agility
  - Advanced access control approaches (ABAC, PBAC, RAdAC, ZBAC, PHABAC…)
- Model-Driven Security (MDS)
  - Tool supported process
  - Model "undistorted" security requirements models at a high level of abstraction,
  - Using other information sources (produced by other stakeholders, expressed in DSL),
  - Transform models into enforceable security rules with little/no human intervention;
  - Run-time decisioning enforcement, dynamic policy updates, policy incident monitoring.

Model-Driven Security (MDS): Automatic generation of technical security rules for information flow enforcement
Use case: Access control, monitoring

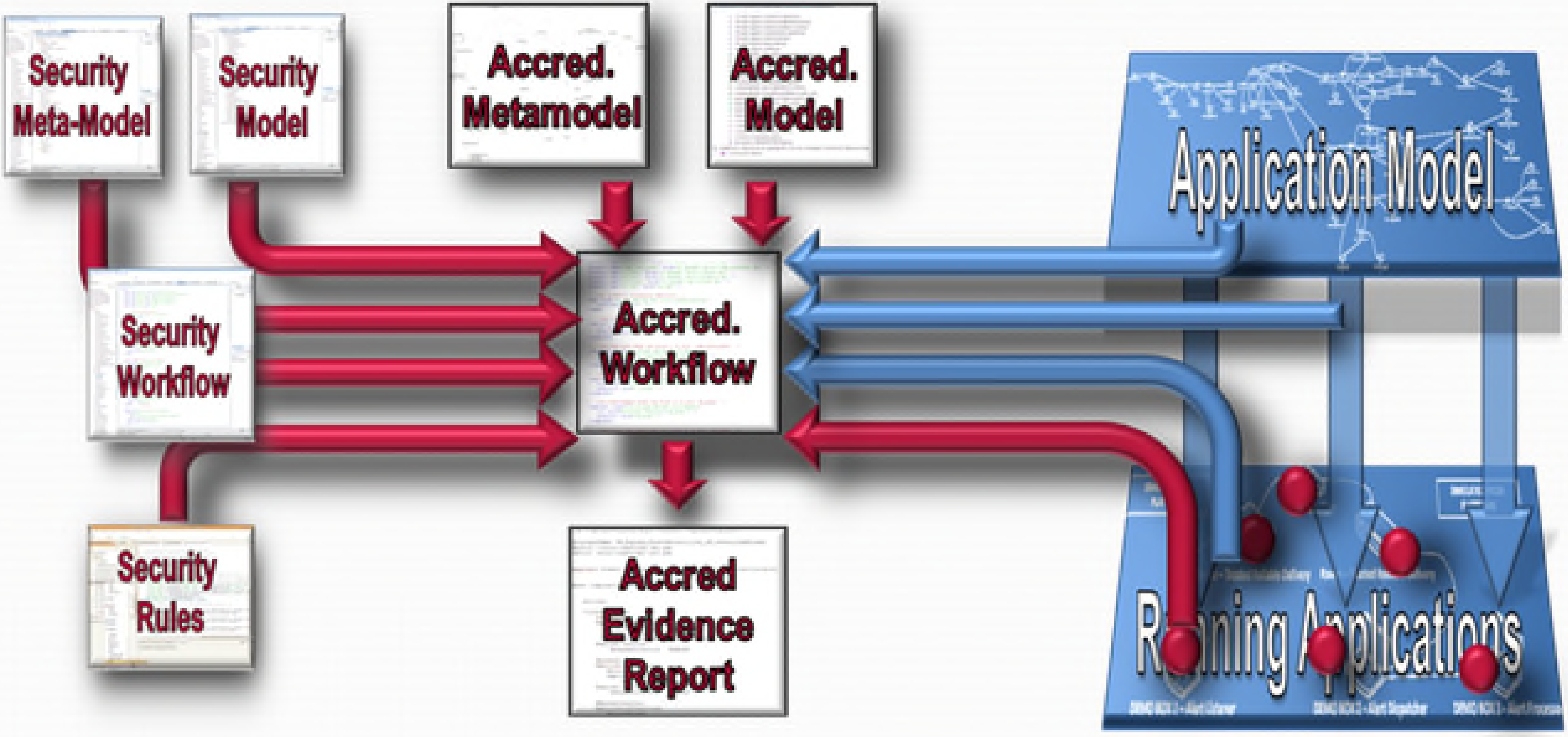
Model-Driven Security Accreditation (MDSA): Automatic generation and update of supporting evidence for info. assurance accreditation (-> *requires MDS)*
Use Case: for Common Criteria

OpenPMF MDS



http://www.youtube.com/watch?v=Eiy19v-n-1s

MDSA



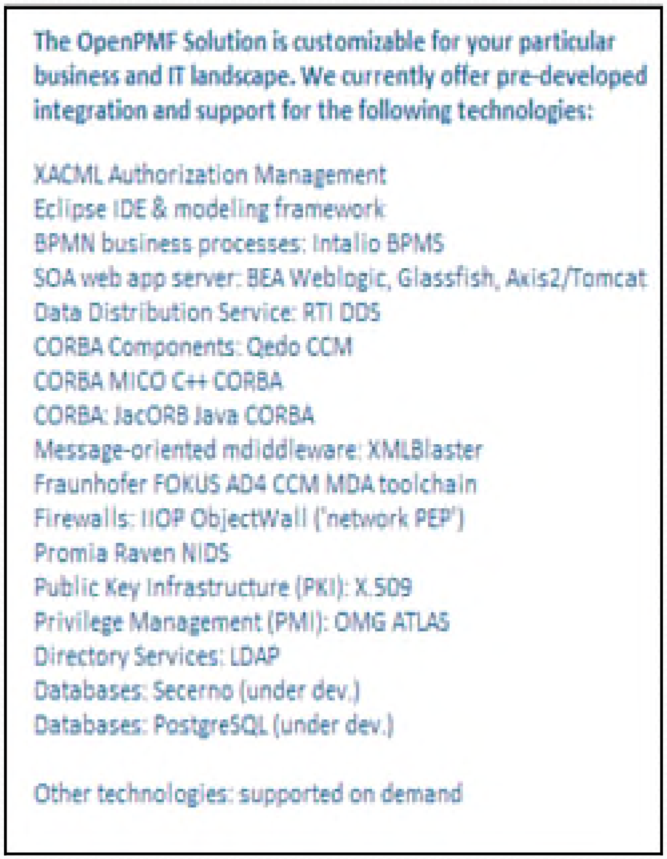
http://www.youtube.com/watch?v=Eiy19v-n-1s

OpenPMF™

OpenPMF is standards-based
(incl. Ecore/MOF, XMI, XACML, ABAC),
award-winning, and patented.

OpenPMF Components

- A model-driven policy authoring tool,
- A model-driven rule generation tool,
- An attribute-based authorization policy server,
- Policy decision/enforcement points,
- A model-driven compliance/accreditation evidence generation tool



The OpenPMF Solution is customizable for your particular business and IT landscape. We currently offer pre-developed integration and support for the following technologies:

XACML Authorization Management
Eclipse IDE & modeling framework
BPMN business processes: Intalio BPMS
SOA web app server: BEA Weblogic, Glassfish, Axis2/Tomcat
Data Distribution Service: RTI DDS
CORBA Components: Qedo CCM
CORBA MICO C++ CORBA
CORBA: JacORB Java CORBA
Message-oriented mdiddleware: XMLBlaster
Fraunhofer FOKUS AD4 CCM MDA toolchain
Firewalls: IIOP ObjectWall ('network PEP')
Promia Raven NIDS
Public Key Infrastructure (PKI): X.509
Privilege Management (PMI): OMG ATLAS
Directory Services: LDAP
Databases: Secerno (under dev.)
Databases: PostgreSQL (under dev.)

Other technologies: supported on demand

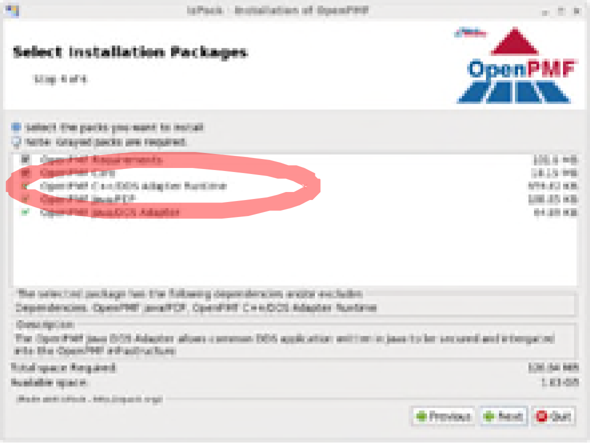
Advanced Access Control

- **Attribute-Based Access Control (ABAC):** Standardized since 2002 …. Now 2015! Adoption: low (?)
  - "attributes: subject, object, requested operations, environment conditions
  - policy, rules, or relationships: allowable operations for a given set of attributes." (NIST 800-162 draft)
- by 2020, 70% of all businesses will use ABAC as the dominant mechanism to protect critical assets, up from less than 5% today (Gartner)
- Example: OASIS XACML

- **Proximity-Based Access Control (PBAC)**
  - policies based on relative proximity/distance
  - between one or more proximity attributes associated with an accessor
  - and one or more proximity attribute associated with an accessed resource. (source: ObjectSecurity)
- Many PBAC dimensions: Geo-Location/Geospatial, Organizational, Operational, Temporal, Business Process, Security, Risk, Social Proximity, Information Proximity, …

- …

MDS & PBAC Example …



IzPack - Installation of OpenPMF

Select Installation Packages

Step 4 of 6

Select the packs you want to install

Note: Grayed packs are required.

☒ OpenPMF Requirements	101.6 MB
☒ OpenPMF Core	18.15 MB
✓ OpenPMF C++/DDS Adapter Runtime	974.42 KB
✓ OpenPMF JavaPDP	108.05 KB
✓ OpenPMF Java/DDS Adapter	64.69 KB

The selected package has the following dependencies and/or excludes:

Dependencies: OpenPMF JavaPDP, OpenPMF C++/DDS Adapter Runtime

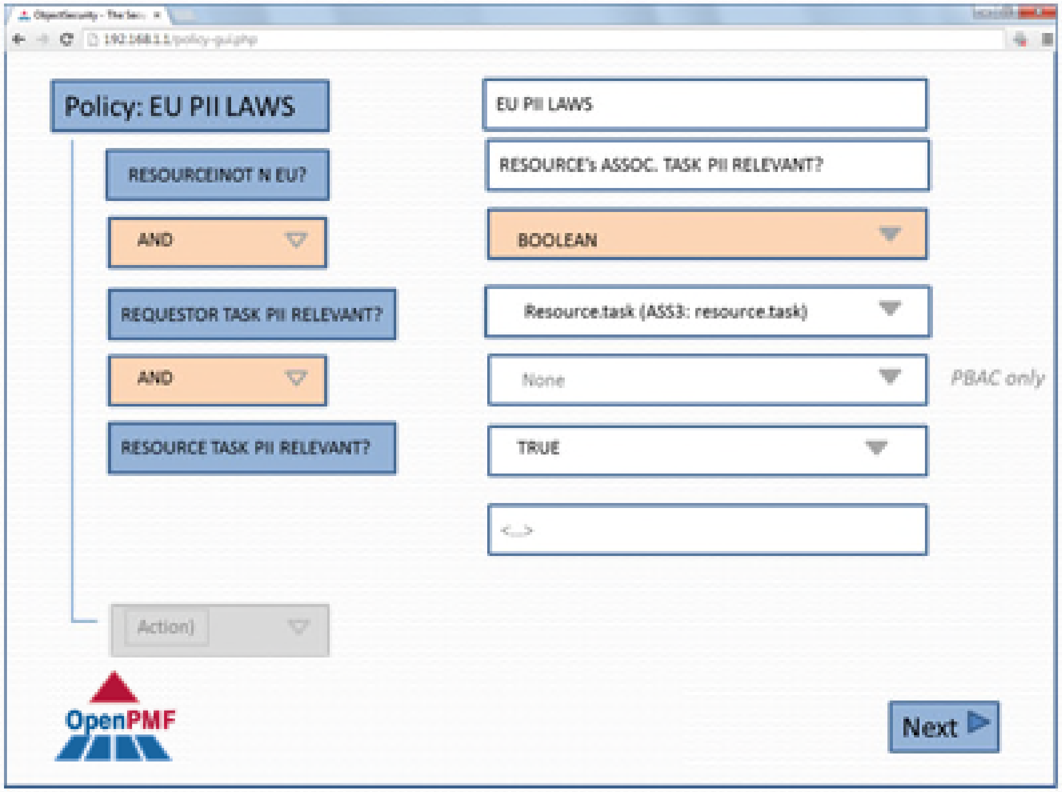
Description

The OpenPMF Java DDS Adapter allows common DDS application written in Java to be secured and integrated into the OpenPMF infrastructure

Total space Required: 120.54 MB

Available space: 1.83 GB

(Made with IzPack - http://izpack.org)

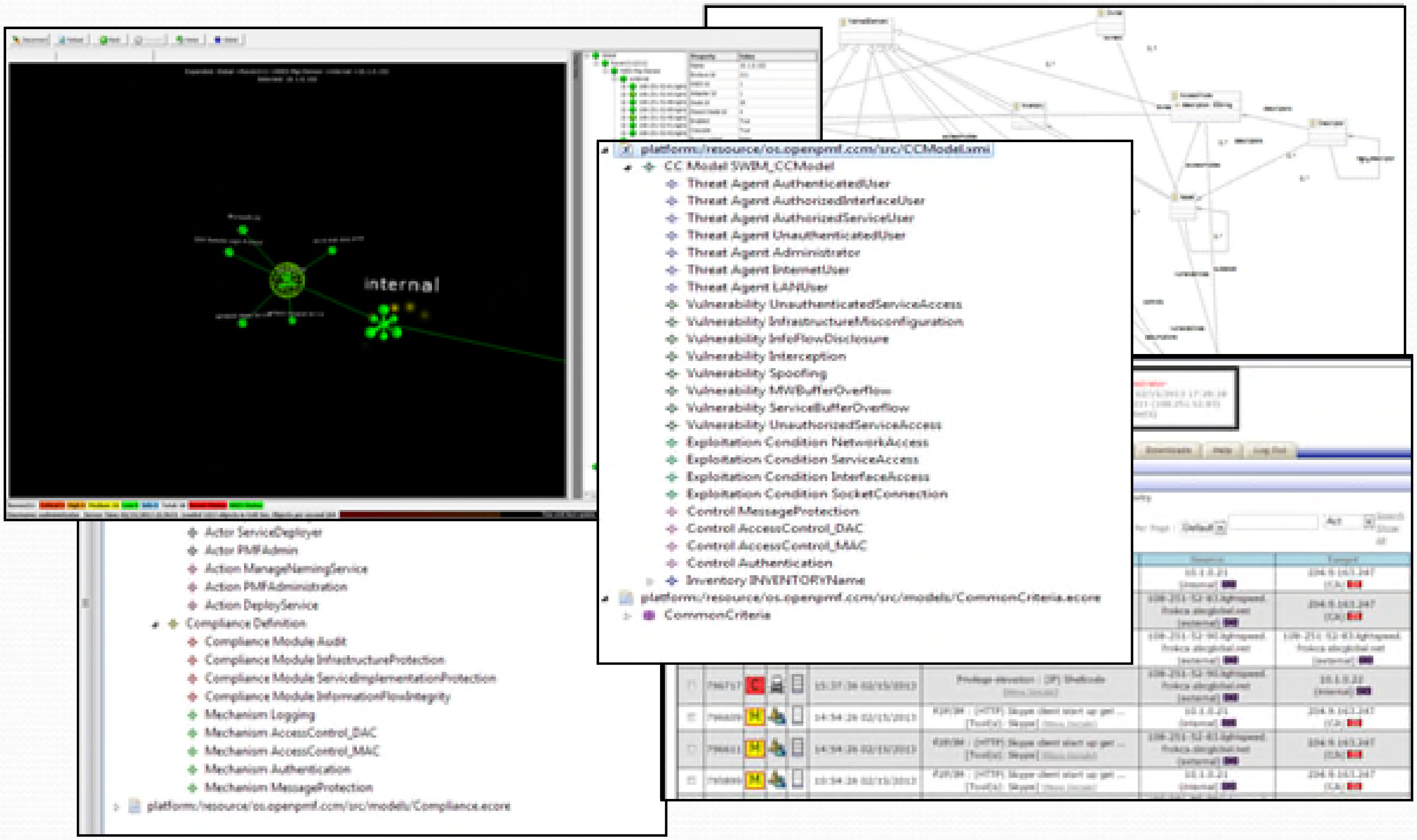


ObjectSecurity - The Sec...

192.168.1.1/policy-gui.php

Policy: EU PII LAWS	EU PII LAWS
RESOURCEINOT N EU?	RESOURCE's ASSOC. TASK PII RELEVANT?
AND	BOOLEAN
REQUESTOR TASK PII RELEVANT?	Resource.task (ASS3: resource.task)
AND	None (PBAC only)
RESOURCE TASK PII RELEVANT?	TRUE
	<...>

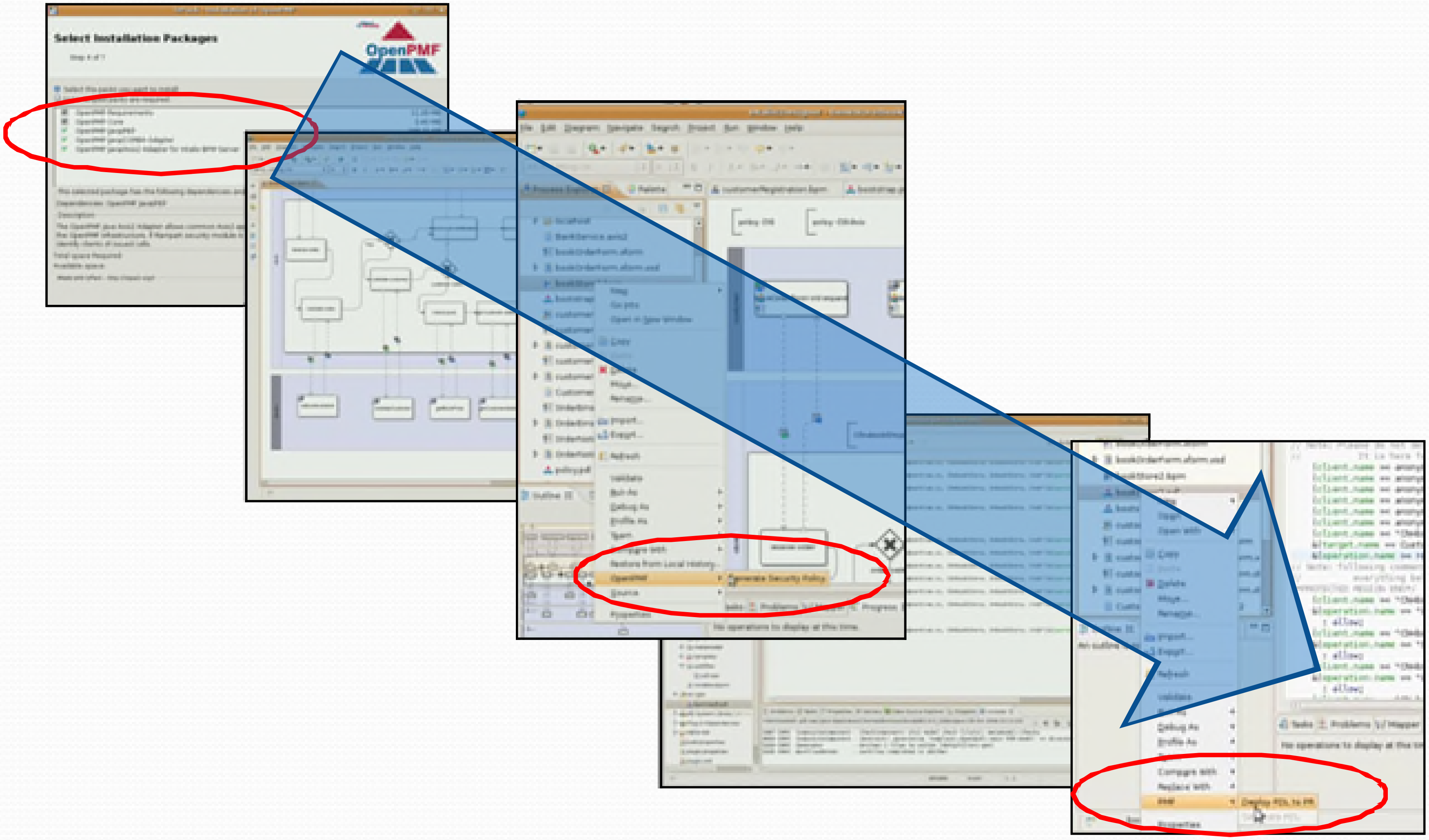
User Experience TrustWand



- platform:/resource/os.openpmf.com/src/CCModel.xmi
  - CC Model SWIM_CCModel
    - Threat Agent AuthenticatedUser
    - Threat Agent AuthorizedInterfaceUser
    - Threat Agent AuthorizedServiceUser
    - Threat Agent UnauthenticatedUser
    - Threat Agent Administrator
    - Threat Agent InternetUser
    - Threat Agent LANUser
    - Vulnerability UnauthenticatedServiceAccess
    - Vulnerability InfrastructureMisconfiguration
    - Vulnerability InfoFlowDisclosure
    - Vulnerability Interception
    - Vulnerability Spoofing
    - Vulnerability MWBufferOverflow
    - Vulnerability ServiceBufferOverflow
    - Vulnerability UnauthorizedServiceAccess
    - Exploitation Condition NetworkAccess
    - Exploitation Condition ServiceAccess
    - Exploitation Condition InterfaceAccess
    - Exploitation Condition SocketConnection
    - Control MessageProtection
    - Control AccessControl_DAC
    - Control AccessControl_MAC
    - Control Authentication
    - Inventory INVENTORYName
- platform:/resource/os.openpmf.com/src/models/CommonCriteria.ecore
  - CommonCriteria

- Actor ServiceDeployer
- Actor PMFAdmin
- Action ManageNamingService
- Action PMFAdministration
- Action DeployService
- Compliance Definition
  - Compliance Module Audit
  - Compliance Module InfrastructureProtection
  - Compliance Module ServiceImplementationProtection
  - Compliance Module InformationFlowIntegrity
  - Mechanism Logging
  - Mechanism AccessControl_DAC
  - Mechanism AccessControl_MAC
  - Mechanism Authentication
  - Mechanism MessageProtection
- platform:/resource/os.openpmf.com/src/models/Compliance.ecore

User Experience Push-Button Automation



Solutions

What “solutions” do we have?

Disclaimer: Not a simple take-home message

The buck stops with the user or buyer?

- inform/educate consumers about cyber-security
- education about security & privacy in schools & jobs to create customers who can discern good from bad
  - users could push buyers
  - buyers could push vendors
  - etc.
- If educated, could request security certifications as part of decision process
- Is this realistic???

The buck stops with the government?

- Education about security & privacy in schools & jobs to create customers who can discern good from bad
- Stick: More regulation (very controversial – but: cf. seatbelts)
  - vendor liability, mandatory breach reporting, best practices regulations, accounting regulations that include security etc.
- Carrot: Financial stimulus into innovation
  - Fund innovators R&D: sometimes good, but hard to get & low ROI
  - Fund adoption of innovation: e.g. smart grid, HITECH: often inefficient.
  - Fund academic research: impact unclear, expensive/inefficient

The buck stops with incumbent vendors?

- would need to play a critical role in innovation adoption.
- unlikely. Will only do the minimum needed
  - to not lose incumbent vendor position against competitors
- few vendors own the lion share of the market
  - Customers support consolidation into few vendors
    - Not conducive to innovation
- could provide security certifications as a marketplace differentiator?

The buck stops with infosec innovators?

- Mostly done today (& ObjectSecurity 2000-2012)
  - bang head against the wall long enough and the "market failure" fails once in a while, i.e. a occasionally small/new/disruptive innovator may make it (die-hard attitude, sweat equity, frustration, patience)
- But:
  - very inefficient, most good ideas evaporate, few rewards for innovative entrepreneurs
  - disgruntles the most valuable stakeholder in the innovation pipeline

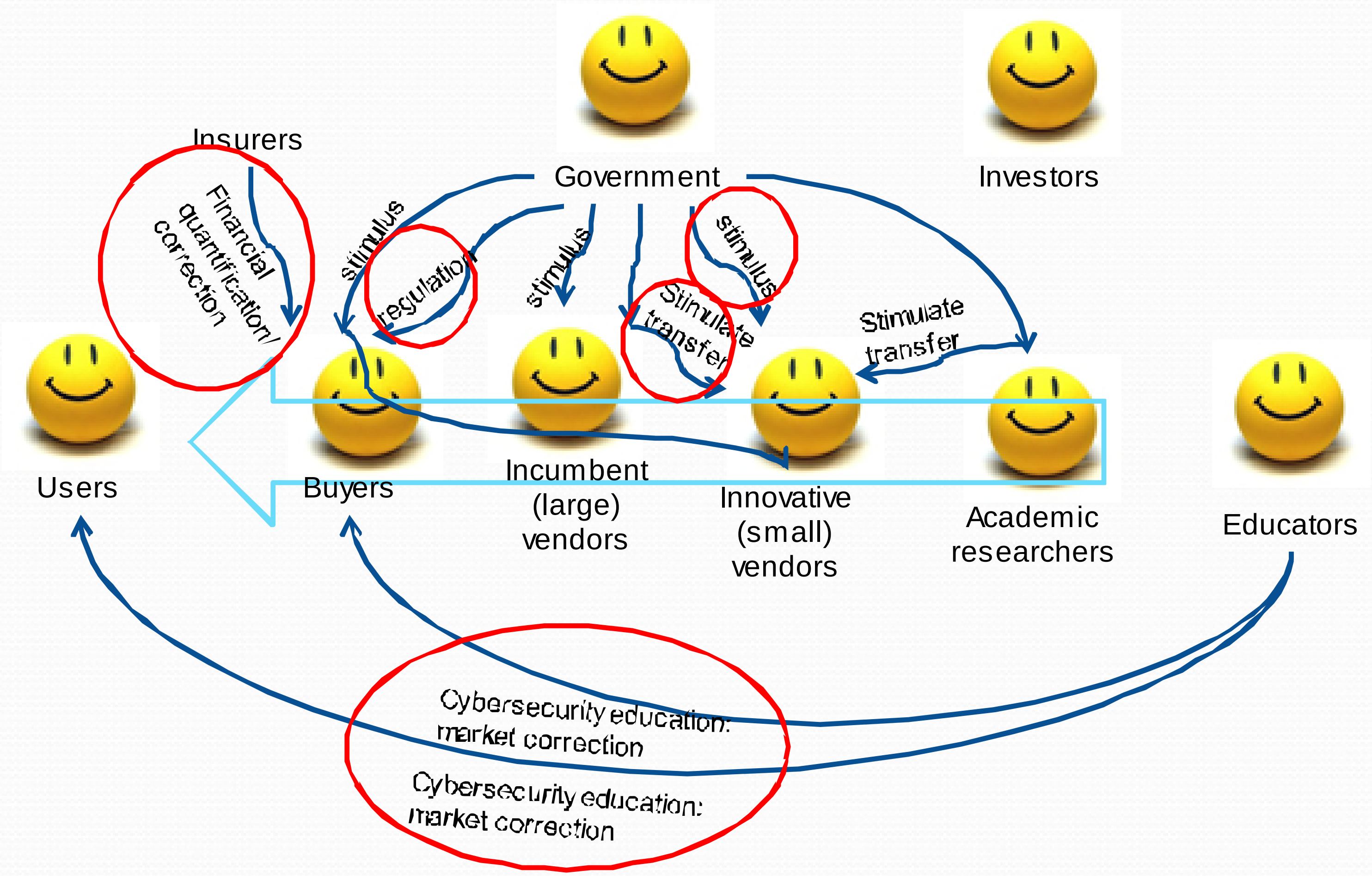
The buck stops with insurances?

- Cyber insurance as a carrot/stick mechanism
- associate a cost (premium) with not doing security well?
  - may mean many security mechanisms are not “worth it”
  - many externalities (e.g. societal damage) are not accounted for
- associate a premium savings with the cost of doing security
  - turns security implementation from cost into a cost-saving
- they don’t insure “stupid”

Or: Wait until it gets bad enough?

- Heard this almost 20 years ago – did not materialize yet
  - Much worse today than predicted back then…
- Maybe we are not that important after all?
  - Who stopped shopping at Target, Home Depot etc.?
- Wait until it's too late? Cyberwar? Massive losses etc.?

In conclusion – where to tune/fix? (just some thoughts)


Insurers
Financial quantification/ correction
Government
Investors
stimulus
regulation
stimulus
Stimulate transfer
stimulus
Stimulate transfer
Users
Buyers
Incumbent (large) vendors
Innovative (small) vendors
Academic researchers
Educators
Cybersecurity education: market correction
Cybersecurity education: market correction

Thank you

Dr. Ulrich Lang, CEO

ulrich-lp@objectsecurity.com

650-515-3391

ObjectSecurity LLC

Disclaimer

The views and opinions expressed during this conference are those of the speaker and do not necessarily reflect the views and opinions held by the ObjectSecurity LLC company, the Information Systems Security Association (ISSA), the Silicon Valley ISSA, the San Francisco ISSA or the San Francisco Bay Area InfraGard Members Alliance (IMA). Neither ISSA, InfraGard, nor any of its chapters warrants the accuracy, timeliness or completeness of the information presented. Nothing in this conference should be construed as professional or legal advice or as creating a professional-customer or attorney-dient relationship. If professional, legal, or other expert assistance is required, the services of a competent professional should be sought.