Modeling eSecurity Risk

Illustrated in the RASCHR-PPP Context

Persistent eSecurity with Automatically Interpreted Policy

Merv Matson, *Chairman and Founder*
RightsMarket, Inc.
MatsonM@RightsMarket.com
(403) 571-1836

Presentation Objectives

- Overview *qualitative* information security risk modeling
- Relate risk modeling to the RASCHR-PPP projects context and beyond
- Understand ‘persistent security’ and how this defense affects the risk model

Qualitative Model

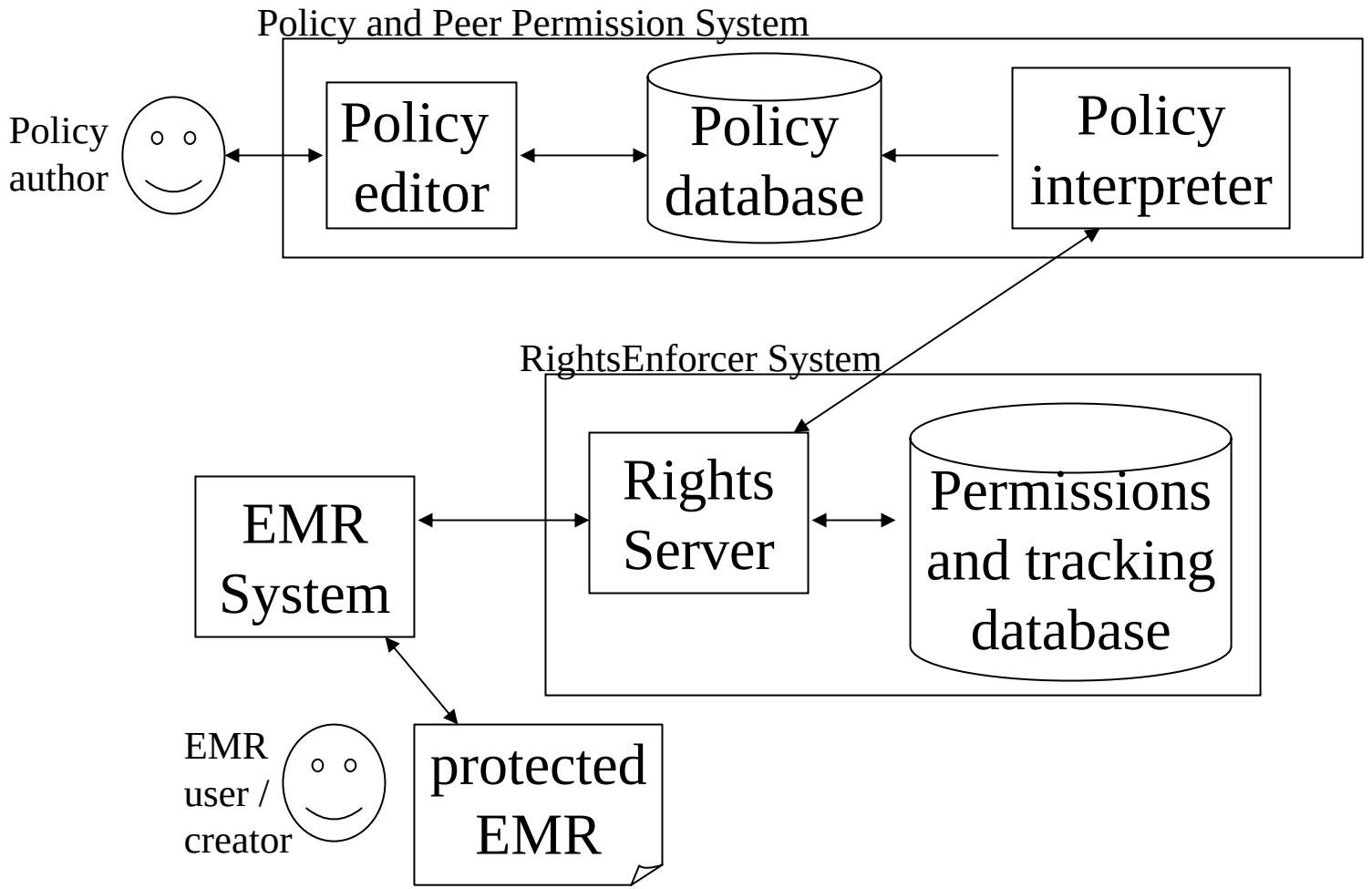
- Choose dimensions of study, analyze to populate/qualify/classify/type
  - System components and states
  - Human actors/roles
  - Risks
    - Mischief: attacks, motivations
    - Accident: modes
  - Defenses
    - Persistent security
- Attach ordinal scale or ranking probabilities
  - Analyze risk dimensions (esp opportunity-time)

Quantitative Model

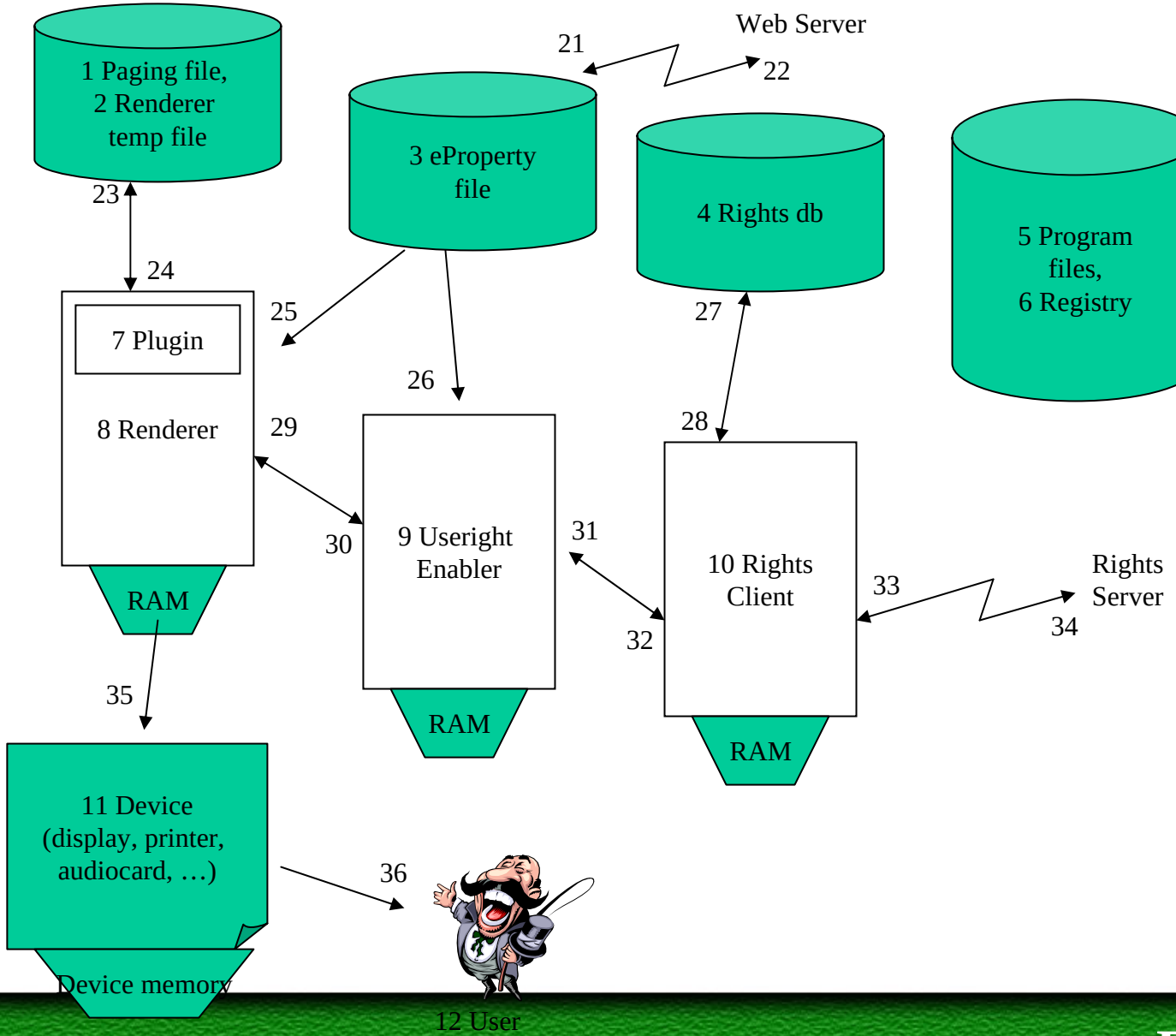
Probabilistic, Financial?

- Attach to qualitative model
  - probabilities of events: $P = \{ p_i \}$
  - loss due to event occurring: $L = \{ l_i \}$
  - therefore, mathematical 'expectation': $\Sigma\ p_i \times l_i$
- Illustration of expectation
  - Consider a dice game: 6$ to roll against the house
  - Payout: 12$ for rolling 1, 3$ for rolling 2-6
  - House's expectation per roll =
    6$ - (1/6 x 12$ + 5/6 x 3$) = 1.5$
- See *Economic Aspects of Information Security*, Gordon and Loeb, www.Rainbow.com (Library)

Components and Actors



RightsClient Threats and Risks Reference Model



RightsMarket

Risks, Examples

- Info accident at
  - client (end user) site
  - server
- Hacker deliberately breaks into the system at
  - client (end user) site
  - server at specific component/state
  - communications node or link
- Legitimate user gone bad

Biggest Risk - Place and Time

- 70 to 80 percent of security breaches came from the internal network; only 6% were deliberate (the Business Information Security Survey 1998, by the National Computing Centre, UK).

Risks, Examples

Intuitively Rated

- Info accident or innocent mishandling at
  - 1 client (end user) site
  - 4 server
- Hacker deliberately breaks into the system at
  - 3 client (end user) site
  - 5 server at specific component/state
  - 8/2 communications node or link
- 100 Legitimate user deliberate malpractice

Dimensions of Risk Analysis

- Opportunity for mischief or accident
  - Place/state and time (duration)
- Mischief motivation
  - Recreational, societal, ideological
  - Revenge, malevolence
  - Financial gain
- Accident modes
  - eMail
  - Shared resource

Opportunity for Mischief or Accident - Place/State

- Opportunity place - the more visible/exposed, or attackable/defenseless, the greater the risk
  - Visible/exposed: File/info is identifiable in the file system, repository, or database with meaningful identifiers
  - Attackable/defenseless: File/info is clear copy (unencrypted)

Opportunity for Mischief or Accident - Time (Duration)

- Opportunity time - the longer time it's vulnerable, the greater the risk
  - Hacker is more likely to find it.
    - Scanning disk
    - Planted spy program looking for use event
  - Careless user is more likely to mishandle it.
    - Wrong eMail attachment
    - Wrong eMail recipient
    - Wrong user on host machine

Mischief Motivation

- Recreational - intellectual challenge, game
- Societal - bragging rights, intellectual or skill achievement
- Ideological - marginalized ‘little guy’ vs. big business, government, institution
- Revenge, malevolence - ‘wronged’ employee, patient, citizen; intention to embarrass
- Financial gain - blackmail, selling selected patient record

Accident Modes

- eMail
  - Wrong attachment
  - Wrong addressee
  - Inclusive address lists
  - Wrong operation, e.g. ‘reply all’
  - Innocent but harmful forwarding
- Leaving EMR in exposed state (egg decrypted)

Risk - Defense

Ref	Exp	Risk - Defense
9	7	See [1] 3.1. Zap calls to URE in eProp - Tamper proofing
10	1	Innocent forwarding and re-forwarding - Persistent eProp security
8	4	Steal shared video memory. - Exclude untrusted apps from simultaneous execution.

Qualitative Model

- Choose dimensions of study, analyze to populate/qualify/classify/type
  - System components and states
  - Human actors/roles
  - Risks
    - Mischief: attacks, motivations
    - Accident: modes
  - Defenses
    - Persistent security
- Attach ordinal scale or ranking probabilities
  - Analyze risk dimensions (esp opportunity-time)

Persistent Security

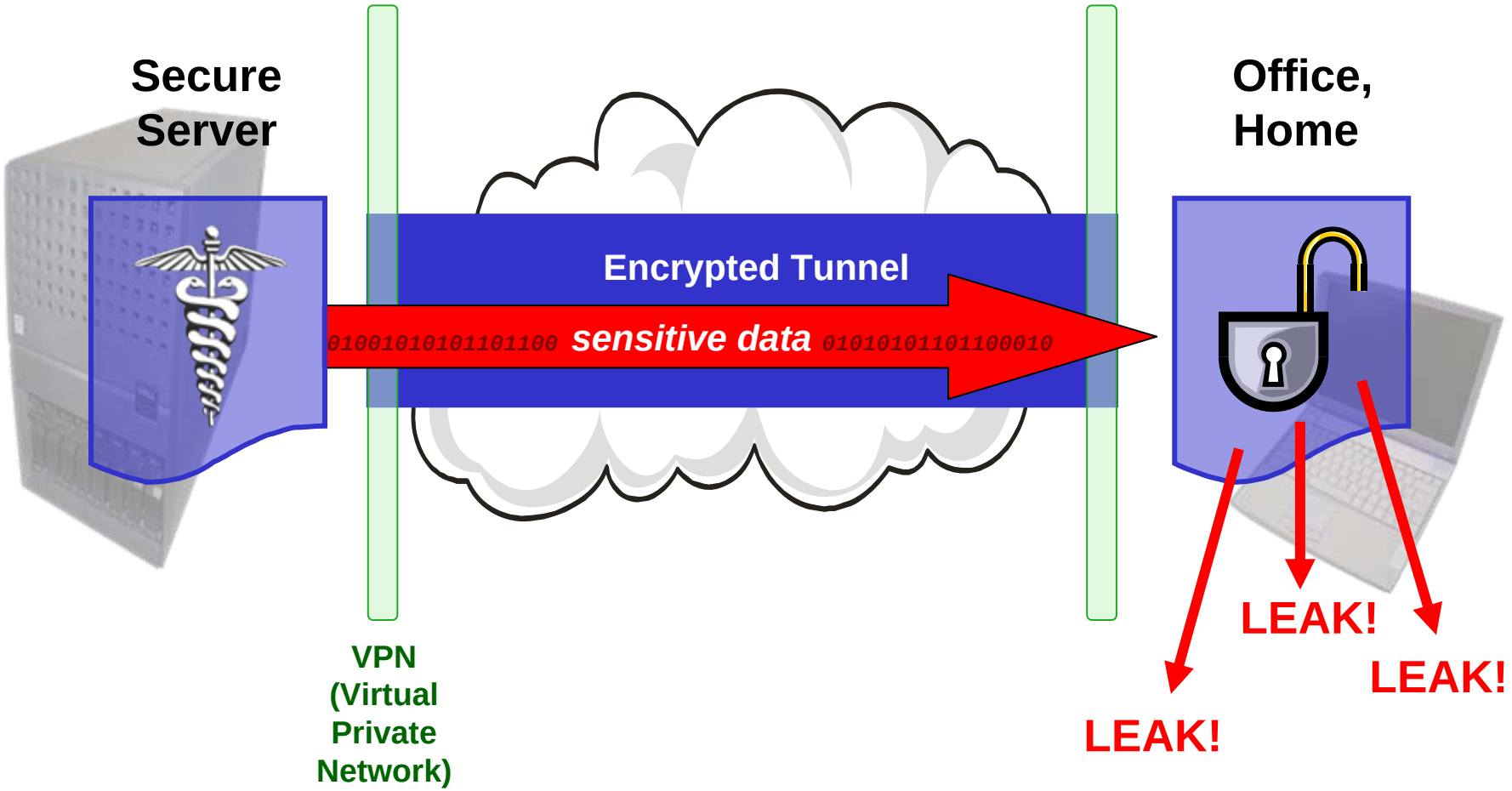
- Extend the reader/renderer program so that
  - It can be trusted to respect policy governing use. It always asks the question “Does this user have the right to do what she is attempting?”.
  - It does not give the user (or hacker) a handle on the decrypted file.
- Security goes with the record, always, like turtle in his shell; not depended on location, like chicken in her cage.

Repository Security

Record is secure behind peripheral defense

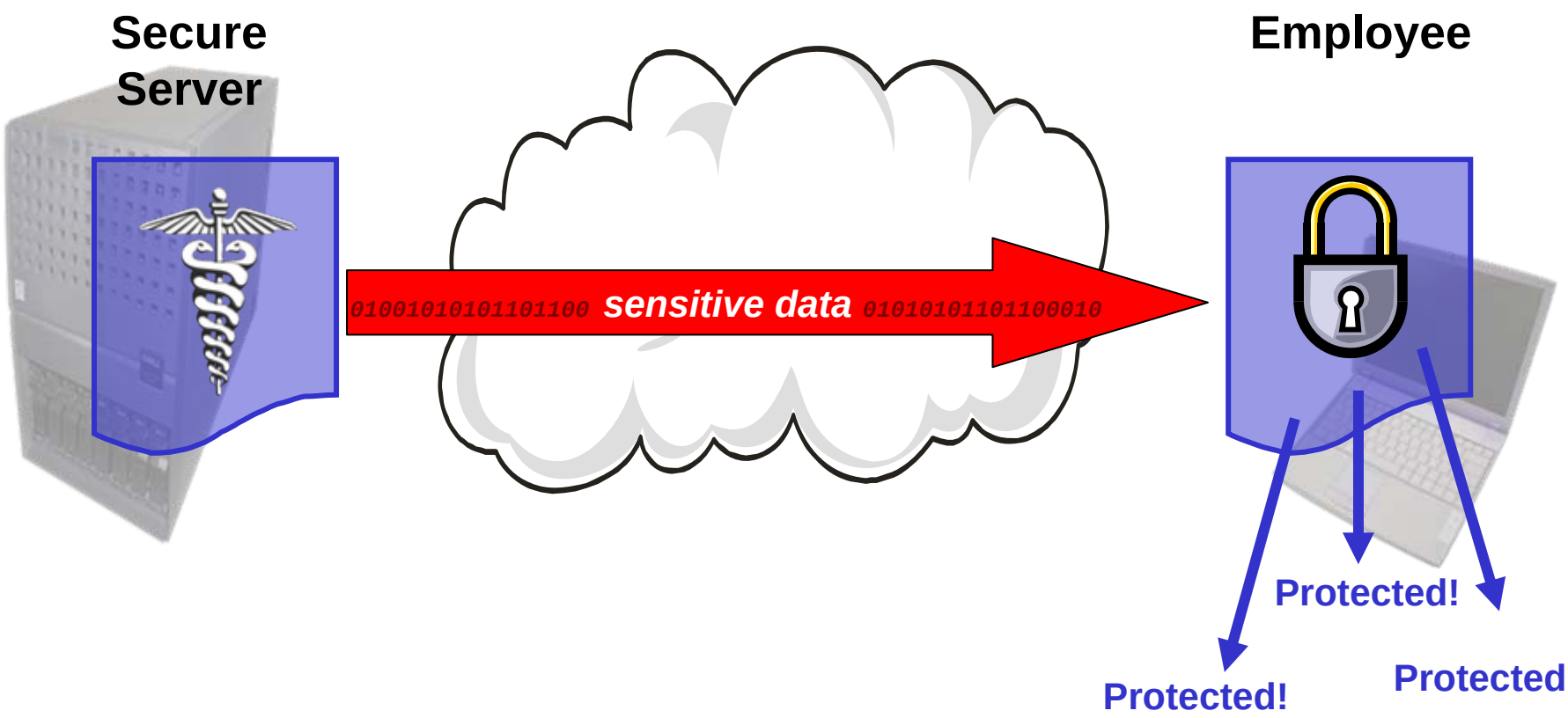
Channel Security

Record is safe during transit



Persistent Security

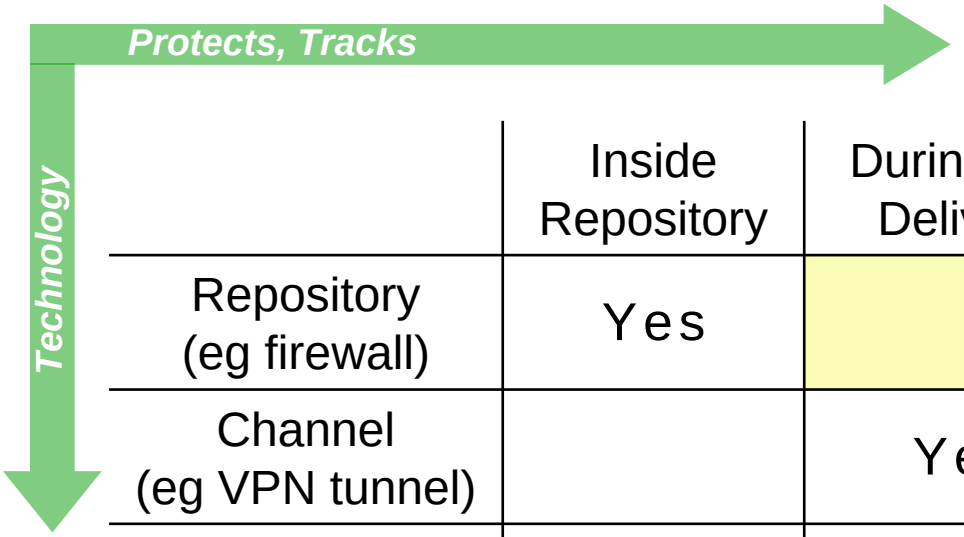
Record is safe at all times, everywhere



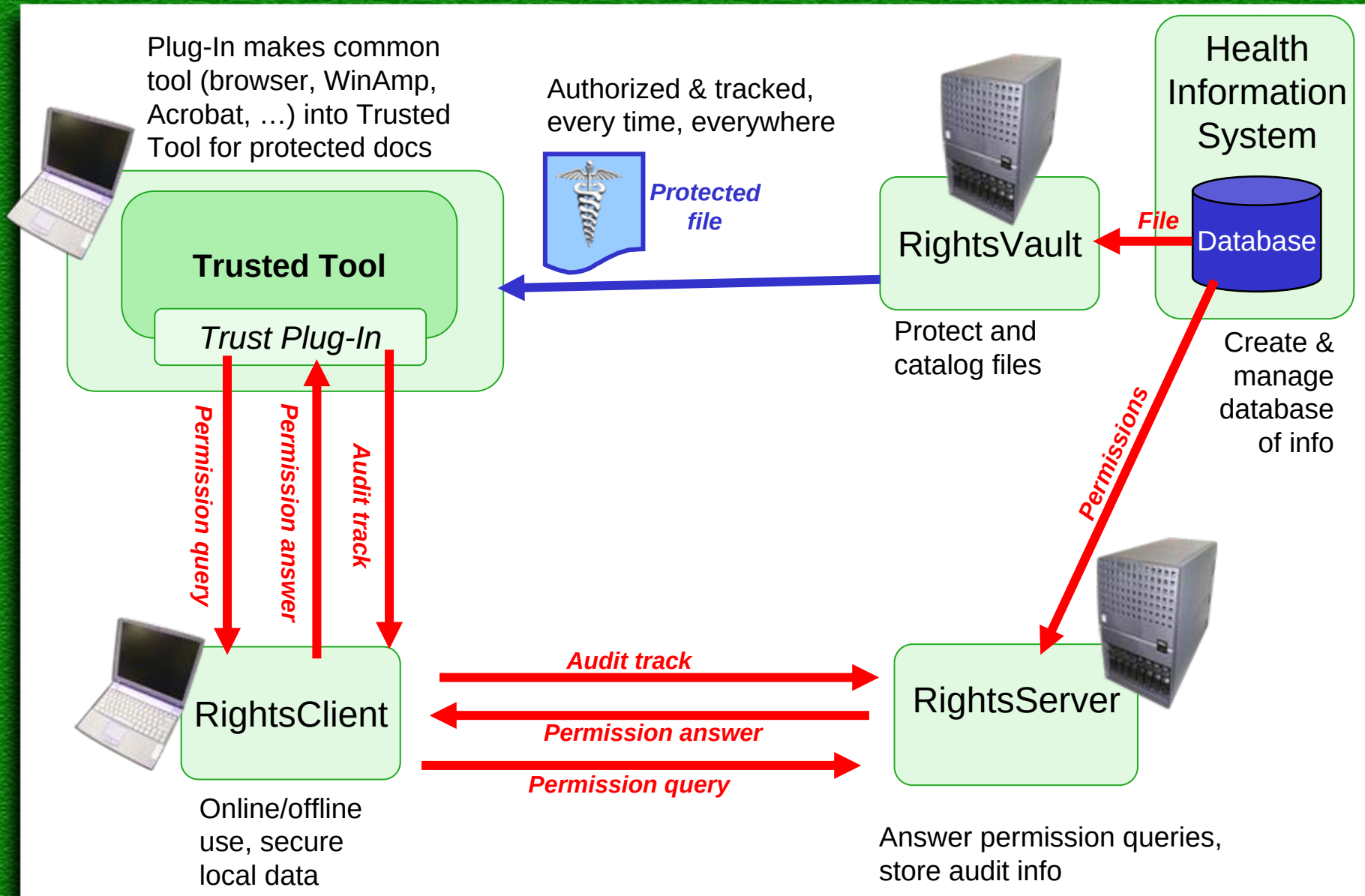
RightsMarket

Not Just Delivery Security

EMR Security & Use Tracking



	Inside Repository	During Net Delivery	Every time, Everywhere
Repository (eg firewall)	Yes		
Channel (eg VPN tunnel)		Yes	
Persistent	Yes	Yes	Yes


Plug-In makes common tool (browser, WinAmp, Acrobat, …) into Trusted Tool for protected docs
Authorized & tracked, every time, everywhere
Health Information System
Trusted Tool
Trust Plug-In
Protected file
RightsVault
File
Database
Protect and catalog files
Create & manage database of info
Permissions
Permission query
Permission answer
Audit track
Audit track
Permission answer
Permission query
RightsClient
RightsServer
Online/offline use, secure local data
Answer permission queries, store audit info

Persistent Security Crunches Risk Opportunity at Point of Use

- The duration of exposure of EMR to accident is reduced drastically
  - Say four orders of magnitude:
    4 x 1/4 hour / 365 x 24 hour = 0.0001
- Same for exposure to hacking
- Permits peer-to-peer (primary care physicians) safe sharing of EMRs, even without common clinical systems

Risks, Examples

Intuitively Rated

- Info accident or innocent mishandling at
  - 1 client (end user) site
  - 4 server
- Hacker deliberately breaks into the system at
  - 3 client (end user) site
  - 5 server at specific component/state
  - 8/2 communications node or link
- 100 Legitimate user deliberate malpractice

Risks, Examples

With Persistent Security, Intuitively Rated

- Info accident or innocent mishandling at
  - 100 client (end user) site
  - 4 server
- Hacker deliberately breaks into the system at
  - 100 client (end user) site
  - 5 server at specific component/state
  - 100 communications node or link
- 100 Legitimate user deliberate malpractice

RASCHR-PPP Context

- Regionally Accessible Cardiac Health Records system
  - Univ Ottawa Heart Institute serving 10 Ottawa area hospitals with cardiac consultations and specialist care
  - RASCHR implements repository security and delivery security between hospitals for defined EMR types; not all
- Policy and Peer Permission system
  - Now under construction, will be installed December with RightsEnforcer (the persistent security components) to secure and facilitate sharing of the other EMR types
  - Expect biggest advantage when the sharing of EMRs is extended out to primary care - combination of persistent security, auto access policy, and use tracking

Questions?