Investigación y desarrollo en seguridad de la información.

Juan G. Lalinde-Pulido

Departamento de Informática y Sistemas

Universidad EAFIT

Agenda

- Conceptos básicos
- Sobre la investigación científica
- La investigación en seguridad informática
- Conclusiones

Conceptos Básicos

- Según el diccionario:
  - Seguridad: calidad de seguro
  - Seguro: exento de todo peligro o riesgo
  - Peligro: Lugar, paso, obstáculo o situación que aumenta la inminencia del daño
  - Riesgo: Contingencia o proximidad de daño

Conceptos Básicos

- La seguridad está soportada en tres vértices:
  - Psicológico: Estado o situación de una persona y su actitud
  - Filosófico: Conjunto de principios establecidos para ordenar la seguridad
  - Real: El sistema, la tecnología y el marco legal

Conceptos Básicos

- En su libro “ABC de la Seguridad Física”, Germán Torres define seguridad como:

  “Conjunto de principios aplicado a un adecuado sistema de protección, unidos a una actitud de obrar en forma lógica y razonable para generar una sensación o estado de tranquilidad real”

  Germán Torres. ABC de la Seguridad Física. Ediciones GATD, 1997.

Conceptos Básicos

- Las distintas ramas de la seguridad se configuran limitando el vértice real.
  - Se habla de seguridad de la información cuando el marco real se limita a la protección de la información en cualquier tipo de representación
  - Se habla de seguridad informática cuando el marco real se limita a la protección de la información cuando es procesada utilizando tecnologías informáticas

Conceptos Básicos

- Algunos principios fundamentales son:
  - La seguridad total es imposible
  - La seguridad es como una cadena: es tan fuerte como el enlace más débil
  - El enlace más débil es, generalmente, el factor humano
  - La seguridad no se obtiene por ocultamiento
  - La seguridad es un proceso

Sobre la Investigación Científica

- Qué es la ciencia?
  - Según la RAE: “Conjunto de conocimientos obtenidos mediante la observación y el razonamiento, sistemáticamente estructurados y de los que se deducen principios y leyes generales.”

Sobre la Investigación Científica

- En las ciencias naturales el objeto de estudio es la naturaleza y se valida (falsea) la teoría al confrontarla con la realidad
- En la ingeniería el objeto de estudio son los objetos artificiales creados por el hombre

Sobre la Investigación Científica

- En informática, la forma de pensamiento es más cercana a las matemáticas que a las ciencias naturales (física, química, etc.)
- Una característica fundamental de la ciencia es que proporciona explicaciones objetivas

La Investigación en Seguridad

- ¿Qué pasa cuando tratamos de aplicar el método científico a la seguridad de la información?
- ¿Se puede hablar de una ciencia de la seguridad?
- ¿Por qué investigar en seguridad de la información?

La Investigación en Seguridad

- Algunos elementos para la discusión:
  - La seguridad no es un problema técnico
  - Es una lucha entre inteligencias
  - Involucra aspectos tecnológicos pero también aspectos sociológicos

La Investigación en Seguridad

- Por la naturaleza de los problemas, la investigación en seguridad es o totalmente teórica o totalmente aplicada.
- Cada uno de estos extremos presenta grandes retos:
  - Teórico: Formalización
  - Práctico: Confidencialidad

La Investigación en Seguridad

- La investigación científica debe buscar principios fundamentales que, al ser aplicados, permitan determinar el nivel de seguridad de la información
- Retos:
  - ¿Cómo se define formalmente la seguridad?
  - ¿Tiene sentido hablar de seguridad?

La Investigación en Seguridad

- ¿Por qué es importante investigar en seguridad?
  - Desde la academia
  - Desde la industria

La Investigación en Seguridad

- La teoría y la práctica se dan la mano.
- Sin conceptos claros, las aplicaciones no pasan de ser simples experimentos.

La Investigación en Seguridad

- Ejemplos:
  - La noción de zona y su uso.
  - Protección criptográfica

La Investigación en Seguridad

- Requiere cooperación
  - Papel de la industria
  - Papel de la academia
- Es requisito fundamental para diferenciarse pues es una industria basada en conocimiento
- Es intensa en capital humano
- Se puede competir en cualquier lugar del mundo

La Investigación en Seguridad

- Limitantes:
  - Información no disponible
  - Aspectos culturales
- Como afrontarla?
  - Formación
  - Cooperación
  - Experimentación

La Investigación en Seguridad

- ¿Qué pueden hacer las universidades?
  - Programas formales con alto nivel científico
  - Grupos de investigación interdisciplinarios
  - Cooperación con la industria
  - Gestión del conocimiento

La Investigación en Seguridad

- ¿Qué puede hacer la industria?
  - Proactividad
  - Cooperación con la academia
  - Redes de colaboración
  - Experiencias aprendidas

La Investigación en Seguridad

- ¿Qué puede hacer el estado?
  - Facilitar la relación academia – empresa
  - Reglamentación
  - Financiar investigación básica
  - Estándares y mejores prácticas

Conclusiones

- Es posible investigar en seguridad, pero requiere cooperación
- Se debe afrontar el tema de manera interdisciplinaria
- La investigación aplicada es útil
- No se debe olvidar la investigación básica