

# Ciencia y software libre

Víctor Leonel Orozco

Centro de Tecnología  
Universidad Federal de Santa Maria

26 de Abril de 2013

# Temática

Difusión científica

Cultura hacker

La nueva cultura de innovación

Consideraciones finales

Referencias

# Objetivos de la difusión científica

- Beneficiar a otros con el conocimiento
- Obtener opiniones de otros
- No reinventar la rueda
- Posibilitar que otros continúen el trabajo

## En capítulos anteriores . . .



Figura : Griegos

## En capítulos anteriores . . .

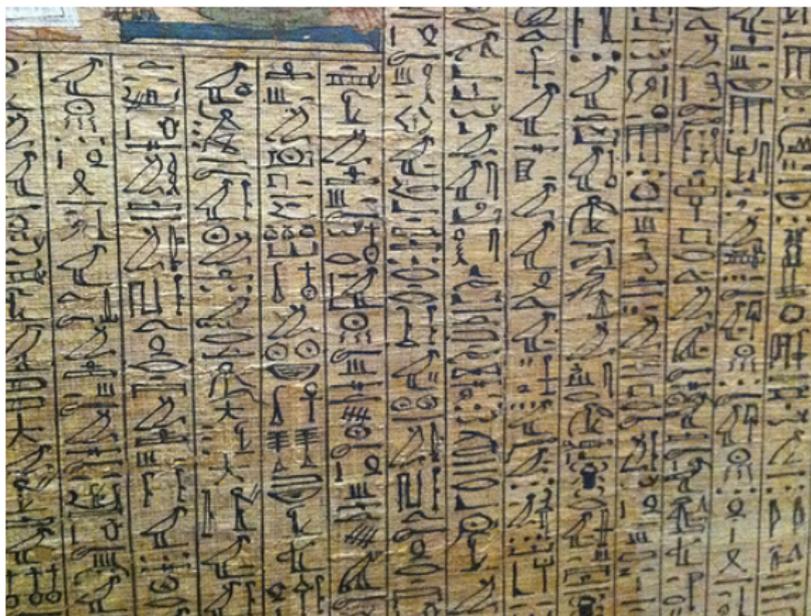


Figura : Egipcios

## En capítulos anteriores . . .



Figura : Mayas

## En capítulos anteriores . . .

- Reservada a los eruditos/escribas/nerds de la antigüedad
- Financiamiento aristocrático
- Curiosidad de quien no necesitaba trabajar y/o tenía un lugar definido en la sociedad

## Cultura libro/paper

- Los doctos necesitaban difundir lo que hacían (sigue siendo un club aristocrático)
- Principalmente estudios religiosos que se derivaron en otras áreas de conocimiento
- Nacen las universidades (Bolonia, Oxford, París, Módena)
- Nacen los libros

## Cultura libro/paper

- Modernización del conocimiento
- Aumentan los libros
- Desiderius Erasmus (Erasmus Mundus)
- Nacen los papers (intros rápidas y concisas)
- Libros: Conocimiento consolidado
- Papers: Conocimiento de punta

# Cultura libro/paper

## Building Situation Awareness to Monitor Critical Infrastructures

Giani Petri, Raul C. Nunes, Victor L. O. Lopez, Tarcisio C. Junior, Osmar M. dos Santos  
Computer Science Graduate Program — PPGI  
Federal University of Santa Maria — UFSM  
{gpetri,ceretta,vlopez,ccolin,osmar}@inf.ufsm.br

**Abstract**—The construction of situational awareness is essential for monitoring critical infrastructures. In this context, we present an application of Endsley's situational awareness model and McGuiness and Foy's extension aiming to build a situational awareness to monitor computer networks infrastructures.

### I. INTRODUCTION

The Internet is becoming essential to society because it helps communication, effective business, commercial transactions and the realization of personal tasks. However, it also makes people and organizations vulnerable to new threats in cyberspace. The Internet and computer networks are considered critical infrastructure [1], so protecting critical information of network traffic is a challenge for organizations.

In this context, the construction of Internet Early Warning Systems (IEWs) was explored by different researches [1] [2]. IEWS aim to detect early threats from the Internet. The monitoring of infrastructures is realized through the construction of situational awareness of the monitored environment (perception of the security situation of network resources), allowing early reactions to malicious events, better control and monitoring of involved resources. Thus, the construction of situational awareness is important to understand events in environments considered as critical.

This work proposes the application of the situational awareness model of Endsley and its extension made by McGuiness and Foy [3] to build situational awareness of computer network infrastructures. A case study conducted in the computer network infrastructure on a higher education institution demonstrates the process of creating situational awareness through the application of the theoretical model on data collected in the institution's network. The construction of situational awareness potentializes the understanding of the activities that occur in the monitored environment and guide the activities of security teams in

awareness is defined by a theoretical model initially proposed by Endsley and later extended by McGuiness and Foy [3]. The extended model is divided into four levels: (i) perception of malicious events; (ii) comprehension of information; (iii) ability to build projections based on historical data and (iv) resolution, where countermeasures are needed to address the identified risks.

Situational awareness is one of the main objectives of an IEWS to monitor critical infrastructures. The architecture of an IEWS consists of various technical components [5]: sensors, knowledge base, and incident response manager, among others. However, the knowledge base constitutes one of the most important technical components, by keeping information that allows more effective actions [5]. Therefore, the construction of situational awareness, which corresponds to an image of the current security situation, will depend on the data stored in the knowledge base.

The construction of situational awareness consists on building the four levels of the theoretical model. In our work, we collected data and conducted a case study in the network infrastructure of the Federal University of Santa Maria (UFSM). The data collected in the monitored environment is stored in the KBAM knowledge base [6] [7]. It represents different essential aspects of computer networks to conduct an effective monitoring.

The case study involved two monitoring points for data acquisition at UFSM: in the network of the admission exam department (Coperves) and in the Data Center network of the UFSM (CPD). In the monitored environments we installed Intrusion Detection Systems (IDS) based on signatures: Snort and Suricata. The integration of data alerts generated by the IDSs was accomplished through the use of the Prelude framework, which allows the unification of various types of applications and sensors. The architecture of the case study also contains a sniffer responsible for quantifying the amount of packets traveling over the network, creating a behavioral pattern. Furthermore, the

## Cultura libro/paper

- Los papers se envían a revistas/congresos
- Un comité evaluó el merito del trabajo (peer-review de PhD)
- El paper es aceptado o rechazado
- Es un proceso costoso y que actualmente requiere de mucho dinero (de .gt solo UFM, UVG y USAC tienen suscripciones a ciertos journals, bastante pobres)
- Una investigación requiere de muchos papers (215)

# Cultura libro/paper

<b>Journal</b>	<b>publisher</b>	<b>\$ per article</b>
Biochemistry	ACS	35
Molecular Biology and Evolution	Oxford Journals	32
Molecular Psychiatry	Nature	32
Nature	Nature	32
Nature Structural and Molecular Biology	Nature	32
American Journal of Human Genetics	ASHG	31.5
Cell	Cell	31.5
Journal of Biological Chemistry	ASBMB	30
Journal of the American Medical Association	AMA	30
Genome Research	CSHL	20
Journal of Bacteriology	ASM	20
Science	AAAS	15
The FASEB Journal	FASEB	12
PNAS	NAS	10

Figura : Costos 2012

# Cultura patente

- 1421 - Felippo Brunellesch - Italia
- 1449 - John de Utynam - Inglaterra
- Evitar la difusión y el lucro con la idea de otro

## Estado 2013

- Limite de acceso al conocimiento por los costos de los papers
- Limite en general por el mal uso de las patentes
- Difusión científica nace abierta y se convirtió en un modelo cerrado solo disponible a aquellos que tengan recursos
- Mantener la estructura de revisión es un proceso complicado
- En América Latina a excepción de Brasil, Chile y más recientemente México y Costa Rica la ciencia no ha despegado ni se considera importante para los gobiernos[1]

# Cultura hacker

- La cultura hacker, nace en las ciencias exactas que desarrollan software (matemática, física, electrónica)
- MIT
- Los programas de computadora solían no tener valor comparado al hardware
- Al volverse el software un negocio (he ahí el patron), se empieza a patentar y limitar el software
- Un barbudo loco no quería imprimir y levantarse de su silla pero Xerox le limita el acceso al software

# Cultura hacker



# Cultura hacker

- Conocimiento vs. lucro
- Innovación de capital vs. innovación colectiva
- Un debate que aun no termina . . .

# FLOSS

- Despego como modelo de desarrollo
- Despego como modelo de libertad
- Despego como modelo de negocios
- Soporte para que la innovación continuara, dando herramientas y creando más herramientas

# FLOSS en ciencia y universidades

- Licencias: MIT y BSD
- Linux (Helsinki), Postgresql(U. Berkley - Ingres), LLVM (U. Illinois Urbana-Champaign), HTTP (CERN), Darwin (Carnegie Mellon - Match), Tex (Stanford), Beowulf (NASA), Lua (PUC-Rio)
- En general el software libre facilita la investigación

# Influencia en la ciencia

- El hijo prodigo regresa a dar lecciones
- Open access
- Creative commons

## Open access

- Acceso libre a las investigaciones científicas
- Europa
- Traslada el costo de revisión de papers al que quiere publicar :(



Figura : Open Access

# Creative commons

- Licencia ampliamente aceptada en trabajos independientes (arte, documentación, wikipedia)
- Revista nature ya permite elegir creative commons [2]



Figura : Creative commons

## Estado actual

- Ambos modelos de innovación coexisten compitiendo entre si [3]
- Los modelos de innovación abierta están siendo ampliamente aceptados en todas partes del mundo, Europa [4], USA [5] y a nuestro nivel en Mexico[6] y Brasil[7]
- Muchas de las personas que contribuyen en Software Libre han sido pioneros en la creación de nuevas ideas y practicas acerca de licenciamiento y propiedad intelectual en los procesos de innovación [8]

## Consideraciones finales

- Actualmente mucha de la ciencia es soportada por software libre o esta generando software libre
- La ciencia jugo un papel fundamental para inspirar la creación de software libre tanto por necesidades tecnológicas, como para acceso al conocimiento
- El software libre encontró el punto para coexistir donde la ciencia aun esta trabajando (merito científico vs. meritocracia por difusión)
- Países como el nuestro tienen una gran oportunidad porque los sistemas académicos ni siquiera existen y no hay que enfrentar resistencia al cambio
- Además el acceso abierto mejoraría nuestro acceso al conocimiento

# Contacto

- <http://tuxtor.shekalug.org>
- [tuxtor@shekalug.org](mailto:tuxtor@shekalug.org)
- <http://github.com/tuxtor/slides>



This work is licensed under a Creative Commons Attribution-ShareAlike 3.0 Brazil License.

# Referencias I

-  R. Latorre, "Science in Latin America: is there hope," *IUPS Newsletter*, 2001. [Online]. Available: <http://www.iups.org/nl3/latorre.pdf>
-  Nature Journal, "License to publish : authors & referees @ npg," 2013. [Online]. Available: <http://www.nature.com/authors/policies/license.html>
-  E. V. Hippel and G. V. Krogh, "Open source software and the "private-collective" innovation model: Issues for organization science," *Organization science*, vol. 14, no. 2, 2003. [Online]. Available: <http://orgsci.highwire.org/content/14/2/209.short>
-  European Commission - Research and Innovation, "Open Access Policy," 2013. [Online]. Available: <http://ec.europa.eu/research/science-society/index.cfm?fuseaction=public.topic&id=1294&lang=1>

## Referencias II

-  Executive Office of the President, “Public Access Memo,” 2013. [Online]. Available: [http://www.whitehouse.gov/sites/default/files/microsites/ostp/ostp\\_public\\_access\\_memo\\_2013.pdf](http://www.whitehouse.gov/sites/default/files/microsites/ostp/ostp_public_access_memo_2013.pdf)
-  A. L. Herrera, “Libre acceso a las investigaciones científicas en internet,” 2013. [Online]. Available: [http://www.youtube.com/watch?feature=player\\_embedded&v=-xtMk-QPzI8](http://www.youtube.com/watch?feature=player_embedded&v=-xtMk-QPzI8)
-  R. Rollemberg, “PLS 387/2011,” 2013. [Online]. Available: [http://www.senado.gov.br/atividade/materia/detalhes.asp?p\\_cod\\_mate=101006](http://www.senado.gov.br/atividade/materia/detalhes.asp?p_cod_mate=101006)
-  G. von Krogh and E. von Hippel, “The Promise of Research on Open Source Software,” *Management Science*, vol. 52, no. 7, pp. 975–983, Jul. 2006. [Online]. Available: <http://mansci.journal.informs.org/cgi/doi/10.1287/mnsc.1060.0560>