



IEEE

CYBER  
SECURITY



# IEEE Cybersecurity Initiative (CybSI)

## Accelerating Innovation in Security & Privacy Technologies

Greg Shannon, IEEE CybSI Chair ( [shannon at cert dot org](mailto:shannon@cert dot org) )  
Chief Scientist, CERT Division,  
Software Engineering Institute at Carnegie Mellon University

23 February 2015

# A Challenge for Engineers



<http://www.dilbert.com/strips/2011-02-03/>

# Today's Presentation

- ▶ Initiative Goal: **Accelerate** innovative research, development and use of **efficient** cyber security & privacy technologies that protect commerce, innovation and expression

# Today's Presentation

- ▶ **Initiative Goal: Accelerate innovative research, development and use of efficient cyber security & privacy technologies that protect commerce, innovation and expression**
  - Overview IEEE & CybSI
  - Center for Secure Design
  - try-cybsi Platform
  - Collaborations

# Overview of IEEE and CybSI

# About IEEE(.org)

**430,000+**  
Members



**38**  
Technical Societies



**160+**  
Countries



**1,300+**  
Annual Conferences



**3,500,000+**  
Technical Documents



**160+**  
Top-cited Periodicals

# About IEEE: Global Standards Developer

- ▶ **Over 900 active standards**
- ▶ **500+ standards under development**
- ▶ **Over 7,000 individual members and 20,000 standards developers from every continent**
- ▶ **200+ entity members**
- ▶ **Working with International standards bodies of ISO, IEC and ITU**
- ▶ **IEEE-SA's process is widely respected and aligns with the WTO and OpenStand principles**



# Security & Privacy Conferences

- ▶ **In 2015, IEEE will hold over 900 conferences touching security and privacy. To note are:**
  - International Conference on Information Systems Security and Privacy (9-11 Feb.; France)
  - **36<sup>th</sup> Annual IEEE Symposium on Privacy and Security (18-20 May; San Jose)**
  - IEEE Conference on Communications and Network Security (28-30 Sept.; Italy)
  - IEEE World Forum on Internet of Things (4-6 Nov.; Switzerland)
  - IEEE International Conference on Identity, Security and Behavior Analysis (23-25 March; Hong Kong)



# Security & Privacy Publications

## ▶ **IEEE Security and Privacy Magazine**

- Provides articles with both a practical and research bent by the top thinkers in the field along with case studies, tutorials, columns, and in-depth interviews and podcasts for the information security industry

## ▶ **IEEE publishes nearly a third of the world's technical literature in electrical engineering, computer science and electronics, including the encryption domain. E.g.:**

- *Performance Analysis of Data Encryption Algorithms*
- *Comparison of Data Encryption Algorithms with the Proposed Algorithm: Wireless Security*
- *Technical Comparison Analysis of Encryption Algorithm On Site-to-Site IPsec VPN*
- *Impact of Wireless IEEE 802.11n Encryption on Network Performance of Operating Systems*
- *Comparative Study of Attribute Based Encryption Techniques in Cloud Computing*
- *Implementation of Advanced Encryption Standards-192 Bit Using Multiple Keys*
- *A Multi-layer Evolutionary Homomorphic Encryption Approach for Privacy Preserving over Big Data*

# IEEE Security-related Standards

Just a sampling:

- ▶ **Encryption (IEEE P1363)**
- ▶ **Fixed & Removable Storage (IEEE P1619, IEEE P1667)**
- ▶ **Printers, copiers, etc. (IEEE P2600)**
- ▶ **Provisions of connectionless user data confidentiality by media access independent protocols (IEEE 802.1AE)**
- ▶ **MAC security key agreement protocol (P802.1Xbx)**

# Cybersecurity Initiative

- ▶ Goal: **Accelerate** research, development and use of **efficient** cyber security & privacy technologies that protect commerce, innovation and expression.

# Cybersecurity Initiative

- ▶ **Goal: Accelerate research, development and use of efficient cyber security & privacy technologies that protect commerce, innovation and expression.**
- ▶ **Activities**
  - Center for Secure Design
  - try-cybsi Platform
  - Collaborations

# Steering Committee

- ▶ **Chair, Greg Shannon, CMU**
  - Network security and anomaly detection
- ▶ **IEEE Fellow, Carl Landwehr, George Washington U.**
  - Cybersecurity “building codes”
- ▶ **IEEE Fellow, Michael Waidner, Fraunhofer SIT & Darmstadt**
  - Security & privacy architectures
- ▶ **IEEE Fellow, Nasir Memon, NYU**
  - Digital forensics
- ▶ **IEEE Fellow, Jeff Jaffe, W3C.org**
  - CEO, HTML standards and security
- ▶ **Jim DelGrosso, Cigital**
  - Project Lead for Center for Secure Design
- ▶ **Jonathan Katz, U. of Maryland**
  - Cryptography
- ▶ **Carrie Gates, Dell Research**
  - Empirical/experimental methods [www.laser-workshop.org](http://www.laser-workshop.org)
- ▶ **Celia Merzbacher, Semiconductor Research (SRC.org)**
  - Hardware
- ▶ **Kathleen Clark-Fisher, Computer Society**
  - Initiative Director for IEEE

# Center for Secure Design



# IEEE CENTER FOR SECURE DESIGN

<http://cybersecurity.ieee.org/center-for-secure-design.html>



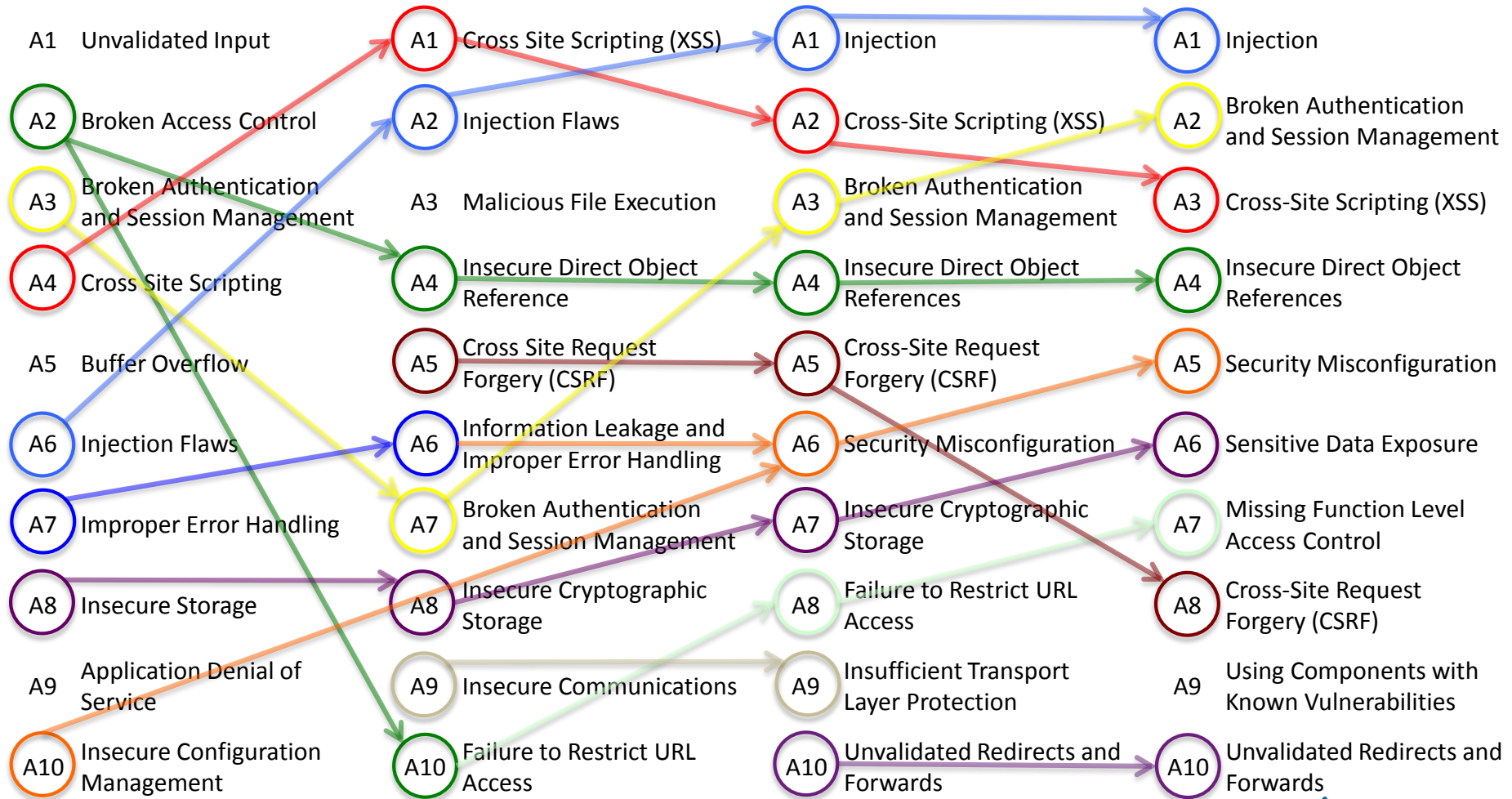
# Patterns in OWASP Vulnerabilities

2004

2007

2010

2013





# Same/Similar Defects For A Decade

- ▶ **Injection Attacks**
- ▶ **Broken Authentication and Session Management**
- ▶ **Cross-Site Scripting**
- ▶ **Security Misconfiguration**
- ▶ **Insecure Direct Object References**
- ▶ **Missing Function Level Access Control**

# Something Needs To Change

- ▶ **We have known about these issues for decades**
  - Knowing != Avoiding
- ▶ **Even when we document these issues, and provide standards describing what to do, that advice is often not followed**

# Avoiding Top Ten Security Flaws (5)

- **Earn or give, but never assume, trust**
- **Use an authentication mechanism that cannot be bypassed or tampered with**
- **Authorize after you authenticate**
- **Strictly separate data and control instructions, and never process control instructions received from untrusted sources**
- **Define an approach that ensures all data are explicitly validated**

# Avoiding Top Ten Security Flaws (5)

- **Use cryptography correctly**
- **Identify sensitive data and how they should be handled**
- **Always consider the users**
- **Understand how integrating external components changes your attack surface**
- **Be flexible when considering future changes to objects and actors**

# Design Flaws Results, Next Steps

## ▶ **Avoiding the Top 10**

### **Software Security Design Flaws**

- Iván Arce, Kathleen Clark-Fisher, Neil Daswani, Jim DelGrosso, Danny Dhillon, Christoph Kern, Tadayoshi Kohno, Carl Landwehr, Gary McGraw, Brook Schoenfeld, Margo Seltzer, Diomidis Spinellis, Izar Tarandach, and Jacob West
- [cybersecurity.ieee.org/images/files/images/pdf/CybersecurityInitiative-online.pdf](http://cybersecurity.ieee.org/images/files/images/pdf/CybersecurityInitiative-online.pdf)
- Spanish Version in March

## ▶ **Workshop on Specific Domains – March 24-26**

- Tools for avoiding flaws
- Consider specific domains: automotive, medical, smart grid, etc.
- Consider Privacy

# try-cybsi Platform

# Understanding Security & Privacy Technologies and Challenges

- ▶ **We've all read or heard about complex technologies, methods and ideas**

# Understanding Security & Privacy Technologies and Challenges

- ▶ We've all read or heard about complex technologies, methods and ideas
- ▶ **Have you wanted to know more beyond reading about it?**



# Understanding Security & Privacy Technologies and Challenges

- ▶ We've all read or heard about complex technologies, methods and ideas
- ▶ Have you wanted to know more beyond reading about it?
- ▶ **Have you tried to use the technology? Reproduce the results? Run the demo?**

# Understanding Security & Privacy Technologies and Challenges

- ▶ We've all read or heard about complex technologies, methods and ideas
- ▶ Have you wanted to know more beyond reading about it?
- ▶ Have you tried to use the technology? Reproduce the results? Run the demo?
- ▶ **Have you had those fail directly? Or fail to help you understand more?**

# try-cybsi Platform

- ▶ **Goal: archive, curate and present:**  
**cyber security & privacy technical artifacts**  
**(code, data, results, exploits, etc.)**  
**AND**  
**cyber security & privacy **experiences** of**  
**those**  
**(examples, demos, experiments,**  
**measurements, evaluations)**

# try-cybsi Platform

- ▶ **Goal: archive, curate and present: cyber security & privacy technical artifacts (code, data, results, exploits, etc.) AND cyber security & privacy experiences of those (examples, demos, experiments, measurements, evaluations)**
- ▶ **try41 Demo**
  - Dendrite example, <https://try.lab41.org>
  - Uses Docker and OpenStack in a private “cloud”
  - In-Q-Tel funded
  - <https://github.com/Lab41/try41>

# try-cybsi Platform

## ▶ Objectives for 2015

- Replicate try41 platform in an accessible cloud
- 12 experiences (containers) available
- 1000 completed user experiences

## ▶ Experience possibilities

- Input fuzzing technique for command line inputs
- Examples of buffer overflow
- Threats mitigated by the new HTST web protocol

# try-cybsi Project Plan

## ▶ Q1 2015

- Project lead and team formed
- Contracts in place or process
- Initial design completed
- Specific cloud selected

## ▶ Q2 2015

- Try41 capability replicated, IOC
- 1 exemplar container created and available for limited use
- Tutorial available for creating and ingesting containers
- 3 containers in development

## ▶ Q3 2015

- try-cybsi platform announced with access to 3 exemplar containers – FOC
- Call for container content creation/submission
- Ingest 3 new containers
- Drive users/viewers to containers via narrow PR

## ▶ Q4 2015

- Ingest 6 new containers
- Solicit and award best content/container
- Drive users/viewers to containers via broad PR

# Want to Participate in try-cybsi?

## ▶ Individual

- Volunteer for the development/operations team
- Create content
- Use content

## ▶ Institution

- Provide the compute platform
- Provide resources to design, develop, instantiate, operate and support

**Contact: [try-cybsi@sei.cmu.edu](mailto:try-cybsi@sei.cmu.edu)**

# Collaborations



# **NSF** –Workshop to Create a Building Code for Medical Device Software Security

<https://sites.google.com/site/bcformdss/home>

**November 19-21, 2014**

**New Orleans, Louisiana**

**Co-organized by C.Landwehr, T.Haigh**



Cyber Security Policy  
and Research Institute

THE GEORGE WASHINGTON UNIVERSITY



# DIMACS/IEEE ESCAPE Workshop

- ▶ **Efficient and Scalable Cyber-security using Algorithms Protected by Electricity (ESCAPE)**
  - @CMU in Pittsburgh, June 10-12, 2015
  - Co-organized by Karl Rohloff, Konrad Vesey
  - Considers the research and engineering implications of an IDA study for the IC: That power (electricity) is the dominate consideration in very large computations
- ▶ **Implication for NITRD is, can access to power be a strategy for constraining cyber threat proliferation?**

# 31 – IEEE Internet Initiative

## ▶ Goals

- Mobilize the IEEE global technical community to support an open, transparent and inclusive participatory Internet governance policy process
- Promote and facilitate the development of trustworthy technology solutions in cyber-security and privacy
- Help connect the IEEE technical community with the policy community to inform and amplify the voice of the technical community in policy discussion venues

## ▶ IEEE Expert in Technology and Policy (ETAP) on Internet Governance, Cybersecurity, Privacy, and Policy

- May Forum co-incident with Oakland Conference
- <http://sites.ieee.org/etap/>

# Further Information

## ▶ Website

- [cybersecurity.ieee.org](http://cybersecurity.ieee.org)
- [cybersecurity.ieee.org/center-for-secure-design.html](http://cybersecurity.ieee.org/center-for-secure-design.html)

## ▶ Email

- Shannon at cert dot org
- kclark-fisher at computer dot org
- try-cybsi@sei.cmu.edu

## ▶ Twitter

- @ieeecybsi (overall initiative)
- @ieeecsd (center for secure design)

Thank You

Questions?