OWASP
HARTFORD
MARCH 2017

HELLO!

I am James McGovern

I am a Whitehat Illuminati Hacker. During the day I moonlight as a Research Director for Gartner. I am here because I love to give presentations. You can find me at @mcgoverntheory

1.

About OWASP

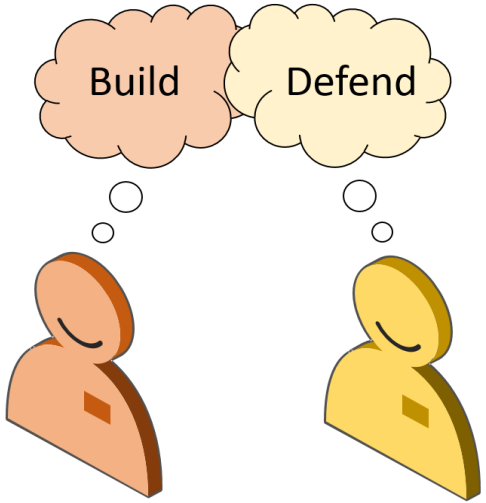
The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of software software. Our mission is to make application security "visible," so that people and organizations can make informed decisions about application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license. The OWASP Foundation is a 501c3 not-for-profit charitable organization that ensures the ongoing availability and support for our work

CORE VALUES

- OPEN: Everything at OWASP is radically transparent from our finances to our code
- INNOVATION: OWASP engoucrages and supports innovation and experiments for solutions to software security challenges.
- GLOBAL: Anyone around the world is encouraged to participate in the OWASP community.
- INTEGRITY: OWASP is an honest, truthful, vendor neutral, global community

Our core purpose is to be a thriving global community that drives visibility and evolution in the safety and security of the world's software.

TWO **WICKED COOL** PROJECTS



Security Shepherd
A web and mobile application security training platform. Security Shephered has been designed to foster and improve security awareness among a varied skill-set demographic.

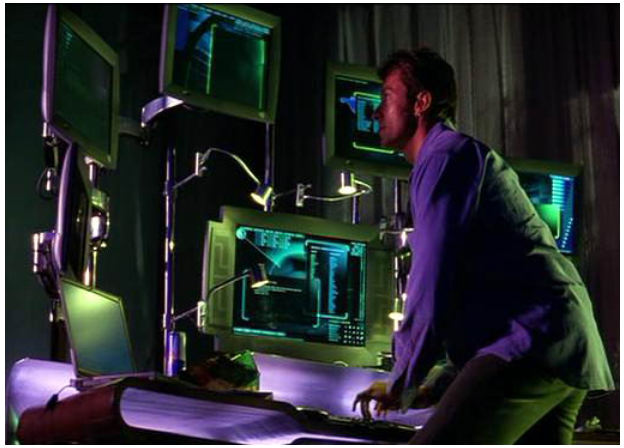
Cornupcopia
A mechanism in the form of a card game to assist software development teams to identify security requirements in Agile, conventional and formal development processes. It is language, platform and technology agnostic.

Oh Hai!

My name is Alvin Fong

I am a “Breaker”. During the day I moonlight as a Business Information Security Officer for Travelers. I hate presentations, but am here because InfoSec has a pipeline problem and you are the solution.
. You can find me on Meetup and LinkedIn

TWO **SWEET** PROJECTS



http://www.unofficial3d.com/files/swordfish02.jpg

Internet of Things (IoT) Project
Designed to help manufacturers, developers, and consumers better understand the security issues associated with the Internet of Things, and to enable users in any context to make better security decisions when building, deploying, or assessing IoT technologies.

OWASP Hartford CT: Pen-testing Lab

- We're creating a capability within the CT chapter that would allow our members to learn and practice ethical hacking skills in a safe environment
- We're creating a forum for practitioners to share techniques and mentor peers in this space

“

Quotations are commonly printed as a means of inspiration and to invoke philosophical thoughts from the reader.

HEALTHCARE SECURITY

A call to action for Medical, Business and Information Security students to work together to secure the healthcare ecosystem.

Business

Enterprise Risk

Cybersecurity Disclosure Act of 2017 (S.536)

- Explain in its SEC filings where expertise exists on their boards and if not why this expertise is unnecessary because other steps taken by company.

Medical

Medicine is a science and thus is data driven

- Collection, analysis and use of data is essential to enabling appropriate diagnosis, treatment, prevent and cure of disease for patient and populations

Technology

Emerging technology is enabling unprecedented change

- Improvements in patient outcomes with reduced costs
- Introduction of incentives and penalties to effectuate desired migration from a fee for service model to a value-based reimbursement solution.
- Involvement of patients with their own data collection

Data privacy and security is a critical concern to providers, payers, patients and regulators

Ever increasing need for international expansion vs. conflicting or varying data privacy, IP and related individual country regulations

Telemedicine

- technology option designed to improve patient health, throughput and patient satisfaction
- includes two-way, real-time and near real-time interactive communication between patient and physician
- decreases costs associated with traditional F2F provision of medical care
- requires appropriate hardware, software, workflow and clinical/practitioner integration

Medical Devices

- Remote diagnostic cardiac monitor (safety, functionality, design control)
- External (Holter, cardiac event, mobile cardiac telemetry)
- Internal (implantable)
- FDA, CE, FCC, etc

- No workable plan to migrate from emerging technology to consistently useful, cost-efficient output for patients, physicians
- Limited and reactionary collaboration between interested parties
- Danger of short-term thinking in a healthcare world currently evolving around emerging and inherently limited life technology
- Healthcare system currently lacks workable/scalable legal and compliance best practices
- Limitation of laws, regulations (FDA, FCC, CMS, HIPAA, etc.)
- Increasing threat of data breaches, hackers, phishing, ransomware
- Intellectual property obstacles

TECHNOLOGY

- Expanded access to information
- Increased engagement

PATIENT VS. CONSUMER

- Patient empowerment
- Curated health and wellness experience

NEXT GENERATION HEALTHCARE

- Heightened provider accountability
- Data-driven fluidity

Product Exploration

- Understand product deployment
- Privacy-by-design
- Product's effect on organization's risk profile

Negotiation

- Vendor's information security program (commercially reasonable; FTC & FDA guidance)
- Address cybersecurity incident responses
- Downstream compliance
- Audit rights
- Representations/warranties and related consequences

Monetization

- Use of IoT in healthcare expected to grow to $117B revenue by 2020
- “Big Data” analytics from health care information could be worth $9 billion to U.S. public health surveillance (by improving detection of and response to infectious disease outbreaks) and $300 billion to American health care in general (McKinsey & Company Data Valuations)
- BUT most organizations have yet to derive significant commercial value
- More than 200 businesses created since 2010 developing innovative tools to make use of available health care analytics
- Companies offer platforms to connect disparate data from across IoT devices for actionable insights (patterns, diagnoses), and turn these into revenue through productized services for external business partners and clients

SECURITY IS AN **ECOSYSTEM**

Manufacturers
Help manufacturers build more secure products in the Internet of Things space.

Developers
Help developers build more secure applications in the Internet of Things space

Consumers
Help consumers purchase more secure applications in the Internet of Things space

YOUR PROFESSOR NEEDS
HOMEWORK

UConn is best positioned to solve healthcare security challenges, but it has to leverage its strengths, connect across “schools” and most importantly think in terms of ecosystems.