RSAConference2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: **ASD-F03**

Game Consoles & Mobile Device Security: A Model for the Internet of Things

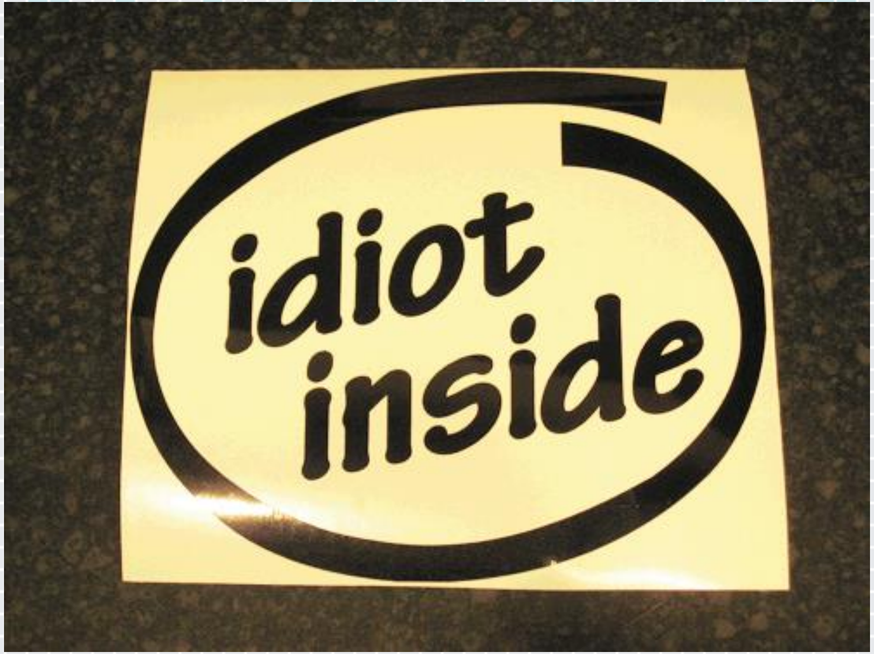
Matt Clapham

Sr. Cyber Security Engineer
GE Healthcare
@ProdSec

#RSAC

Agenda

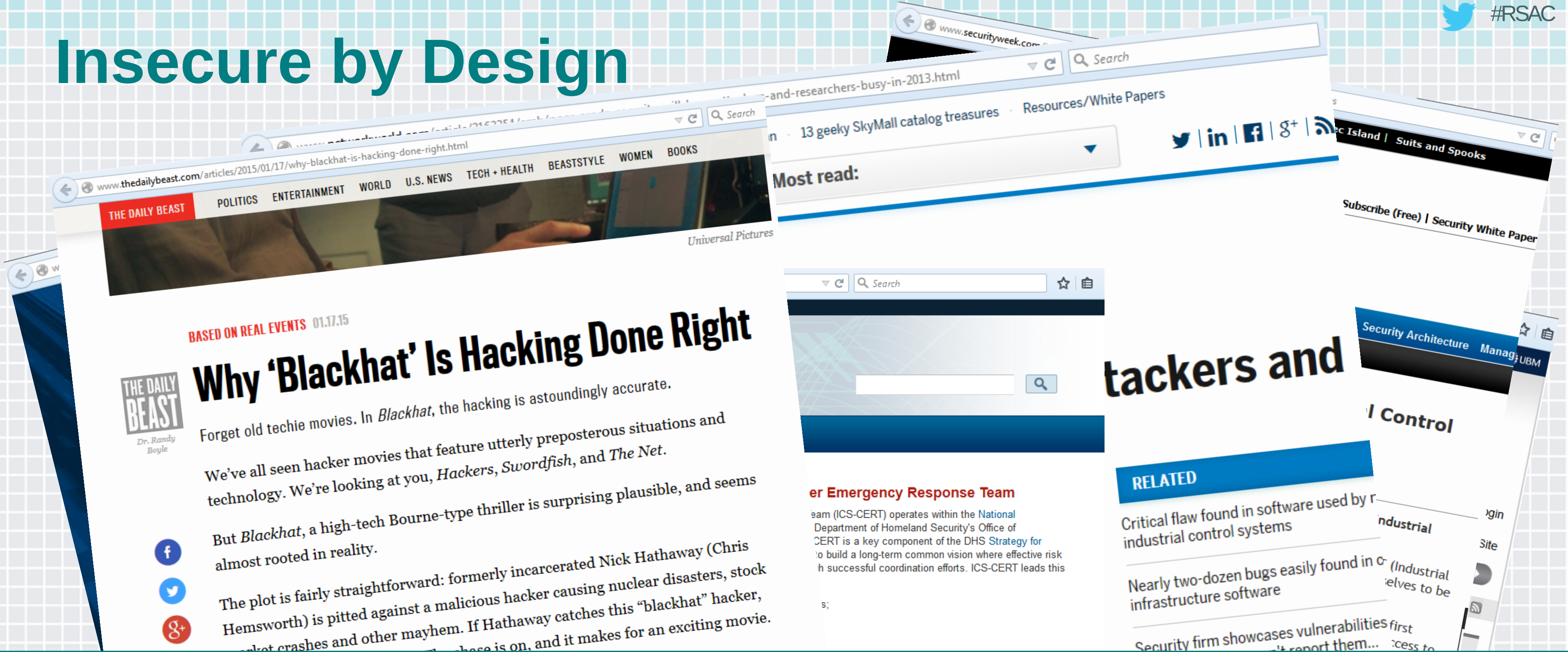
- Description of IDIoTs
- How it got this bad
- What we can learn from game consoles and smart phones
- Comparison, contrast, and pulling it together
- Applying it



Industrial Device Internet of Things

IDIoTs

Insecure by Design



www.securityweek.com

-and-researchers-busy-in-2013.html

13 geeky SkyMall catalog treasures · Resources/White Papers

Most read:

www.thedailybeast.com/articles/2015/01/17/why-blackhat-is-hacking-done-right.html

THE DAILY BEAST POLITICS ENTERTAINMENT WORLD U.S. NEWS TECH + HEALTH BEASTSTYLE WOMEN BOOKS

Universal Pictures

BASED ON REAL EVENTS 01.17.15

Why 'Blackhat' Is Hacking Done Right

Forget old techie movies. In *Blackhat*, the hacking is astoundingly accurate.

THE DAILY BEAST
Dr. Randy Boyle

We've all seen hacker movies that feature utterly preposterous situations and technology. We're looking at you, *Hackers*, *Swordfish*, and *The Net*.

But *Blackhat*, a high-tech Bourne-type thriller is surprising plausible, and seems almost rooted in reality.

The plot is fairly straightforward: formerly incarcerated Nick Hathaway (Chris Hemsworth) is pitted against a malicious hacker causing nuclear disasters, stock market crashes and other mayhem. If Hathaway catches this "blackhat" hacker, the chase is on, and it makes for an exciting movie.

er Emergency Response Team

eam (ICS-CERT) operates within the National Department of Homeland Security's Office of CERT is a key component of the DHS Strategy for o build a long-term common vision where effective risk h successful coordination efforts. ICS-CERT leads this

tackers and

RELATED

Critical flaw found in software used by industrial control systems

Nearly two-dozen bugs easily found in infrastructure software

Security firm showcases vulnerabilities first ...n't report them...

c Island | Suits and Spooks

Subscribe (Free) | Security White Paper

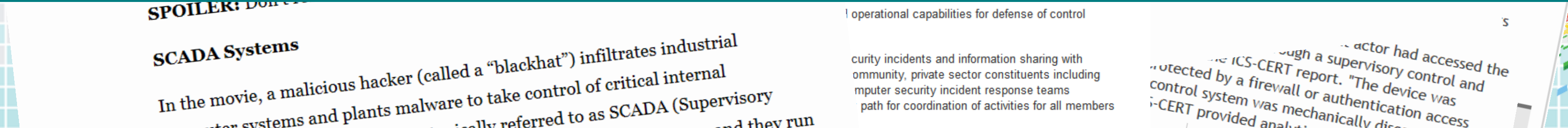
Security Architecture Manag UBM

l Control

ndustrial (Industrial elves to be first cess to

gin Site

> "There are no security elements in the Modbus protocol, over serial or TCP communications." - digital bond



SPOILER: Don't

SCADA Systems

In the movie, a malicious hacker (called a "blackhat") infiltrates industrial ...tor systems and plants malware to take control of critical internal ...ally referred to as SCADA (Supervisory ... and they run

operational capabilities for defense of control

curity incidents and information sharing with ommunity, private sector constituents including mputer security incident response teams path for coordination of activities for all members

...actor had accessed the ...ugh a supervisory control and ...e ICS-CERT report. "The device was ...otected by a firewall or authentication access control system was mechanically dis... -CERT provided analyti...

Your Firewall

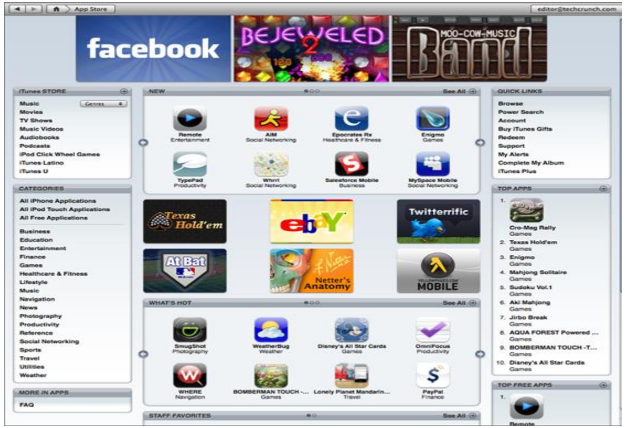
“NOT RESPONSBILE FOR FIRE OR THEFT”

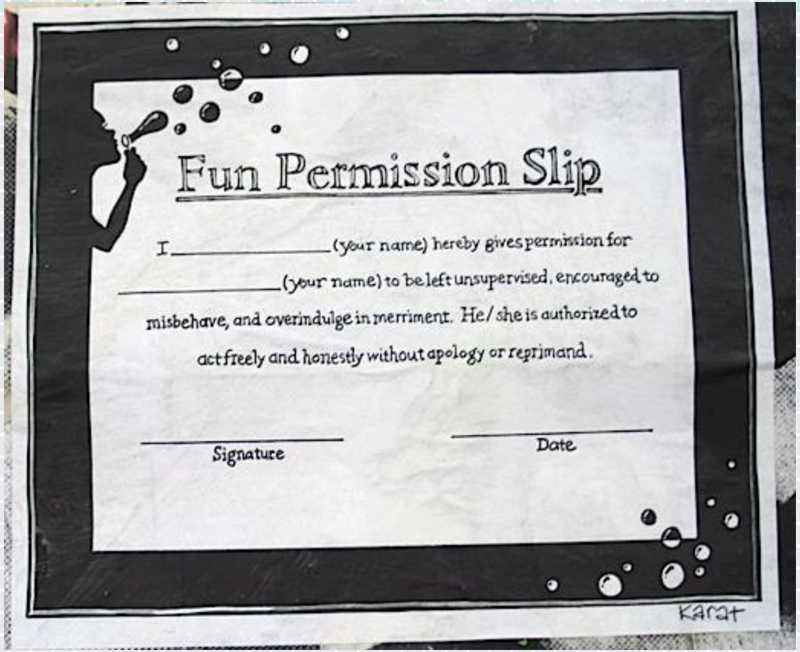
Tools

Leverage lessons from others' fail.

Everything You Wanted to Know About Game Consoles But Were Afraid to Ask

All I Really Need to Know About App Stores I Learned from Smart Phones





Fun Permission Slip

I ______________ (your name) hereby gives permission for ______________ (your name) to be left unsupervised, encouraged to misbehave, and overindulge in merriment. He/she is authorized to act freely and honestly without apology or reprimand.

______________ Signature

______________ Date

Karat

Capabilities

Mom said you could do it.

Whitelisting

The bouncer for your platform.

No Silent Failures

“Danger, Will Robinson! Danger!” – Robot from *Lost in Space*

Services

Are you being served?

Security Life Stages

IDIoTs

Game Consoles & Smart Phones

Tying it Together in Summary

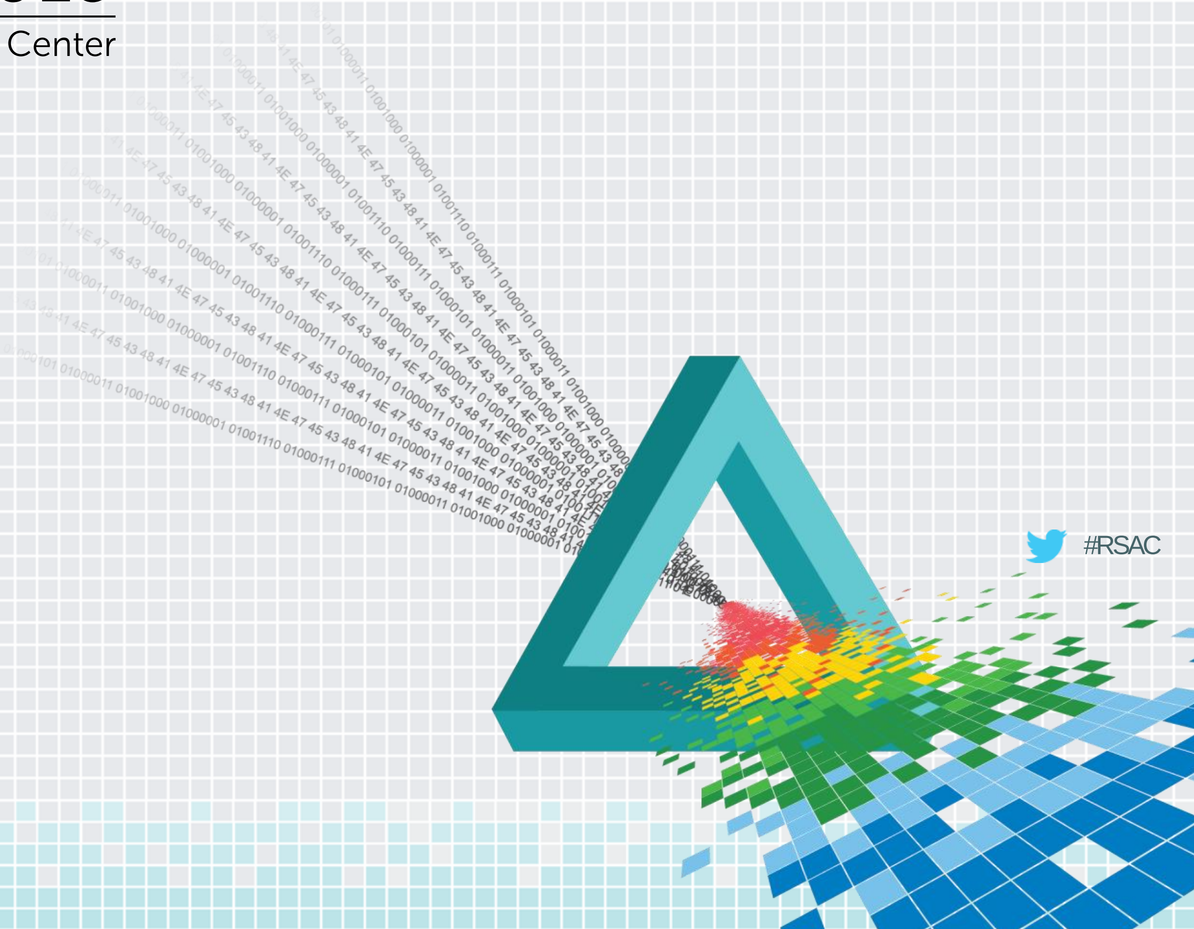
Turning crazy into actionable.

Applying These Concepts

- In the next week…
  - Identify a target product under development for security improvement
- In the next 3 months…
  - Build a threat model for the product
  - Design mitigations for identified problems
- In the next 6 months…
  - Add Static analysis for security problems into the build cycle
  - Make fixing static analysis security problems a check-in requirement

Customers assume security is present in the product.

Don’t prove them wrong.



Thank you