OSIsoft®

USERS CONFERENCE 2016

April 4-8, 2016 | San Francisco

TRANSFORM YOUR WORLD

Bow-Tying It All Together: Analyzing Your Attack Surface

Bri Rolston

GkJuju Security Consulting

April 2016

Geek Juju?

- ICS Security Lead at Monsanto
- Any experience in cyber security?
  - Security operations
  - Code security
  - Incident response
  - Telecomm security
  - Threat management
- Any experience in ICS?
  - Idaho National Laboratory (INL)
  - DoD, DHS, and DOE CIP experience
  - Kimberly-Clark Corporation

Technical Biases

My hat is blue….

- If they can attack it, we can defend it.
- Breaker not a maker
- Where my thoughts tend to wander….
  - Trends in malware use & creation
  - Analyzing attack surface
  - Fingerprinting attack teams

Shifting Threat Perspective

Threat from industry perspective

- Operational risk
  - Risk = f (Probability, Impact)
- Priorities
  - People
  - Process
  - Technology
  - Security
- More on this in previous research
  - Attack Technology Analysis & Characterization (ATAC)
  - Response Analysis Characterization & Tools (ReACT)

Starting with the ATAC

They attack. I defend. Shiny object!

- **Cyber defense would be more EFFICIENT if I**
  - Stop defending all targets the same way
  - Identify the high value targets on my network first
  - Evaluate the attack surface
- **Tools used**
  - Reversing off the target (software patent)
  - ATAC (attack styles, FSL, ATAC Life Cycle)
  - ReACT (ASA, ASE, FSM)

Attack Planning

Technology is a tool people use to get work done and to solve business problems.

Adversaries	Attack Work Flow	Attack Technology
• Have operational goals • Are creatures of habit • Solve problems uniquely • Plan attacks based on previous factors	• Makes it possible to characterize threat • Describes the life cycle & work • Drives selection of attack tech	• Shows how adversary solves problems • Can be used to identify most likely attack paths
ATTACK STYLE		

ATAC Life Cycle

Hackers have project managers, too.

Target Development	Exploitation & Pivoting	Attack Operations	Attack EoL
Design	Implementation	Maintenance	EoL

• Work planning
• Identify ops goals
• Develop attack strategy
• Create tool kit
	• Point of Entry (PoE)
	  • Foothold
	  • Elevate privilege
	• Pivot to next system
		• Achieve ops goals
		• Shift in technical focus
		• Different technical needs than E&P
		• Lots of infra.
			• End of technical work

• Network mapping • Vuln scanning • Spear-phishing	• 0-days • Pass the hash • Elev. of Priv. (EoP)	• C&C channels • Keystroke logging • Remote admin	• Clean up

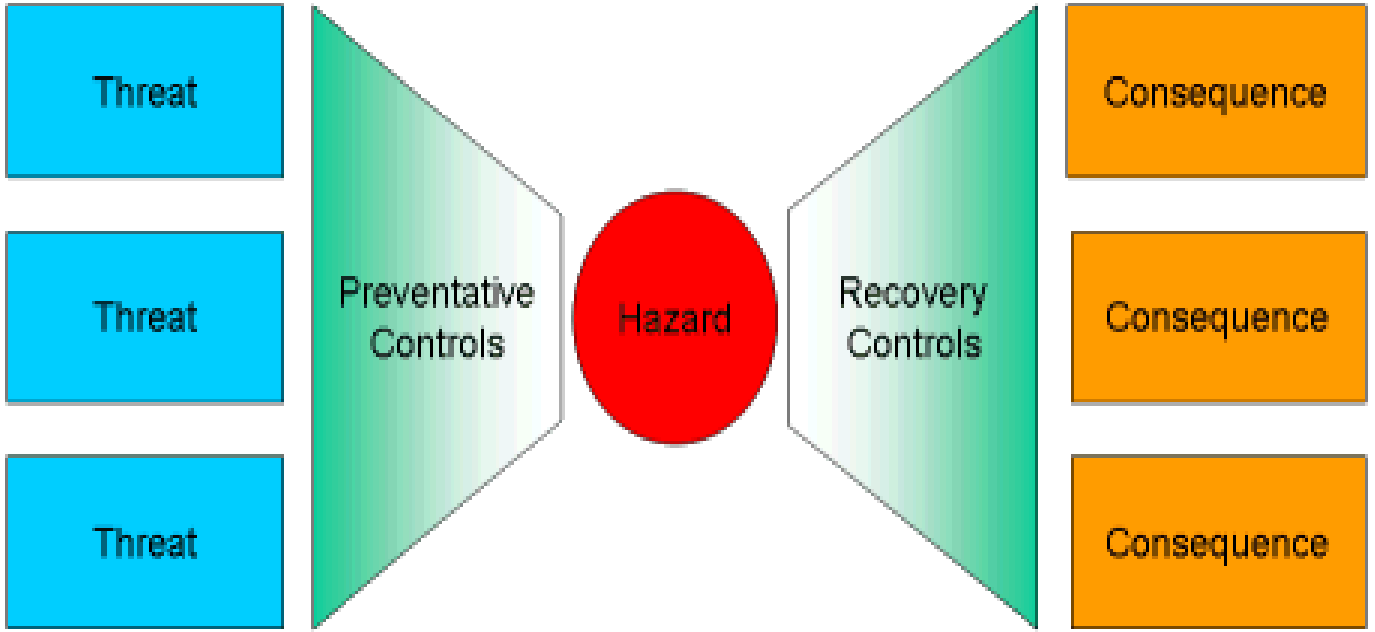
ATAC FSM = Epic Fail

It's not you. It's me.

- ATAC FSM not easily understood
- Threats, attack vectors, 0-days….Oh, my!
- Reboot my comms
  - Makers not breakers
  - ICS types not hackers
  - C-suite not geeks

OSIsoft's Idea: Bow Tie Analysis

Common risk analysis method



Reboot

ATAC + Bow Tie Analysis

- Threat analysis
  - Stuxnet 0-day
  - Print spooler attack
- Apply it to PI Server

Mitigating Cyber Risk

ATAC + Bow Tie Analysis

- Attacker's goal
  - Start as remote unauthorized user
  - Open a "door" on the system
  - Elevate privilege to admin on PI Server
- Defender's goal
  - Mitigate cyber security risk

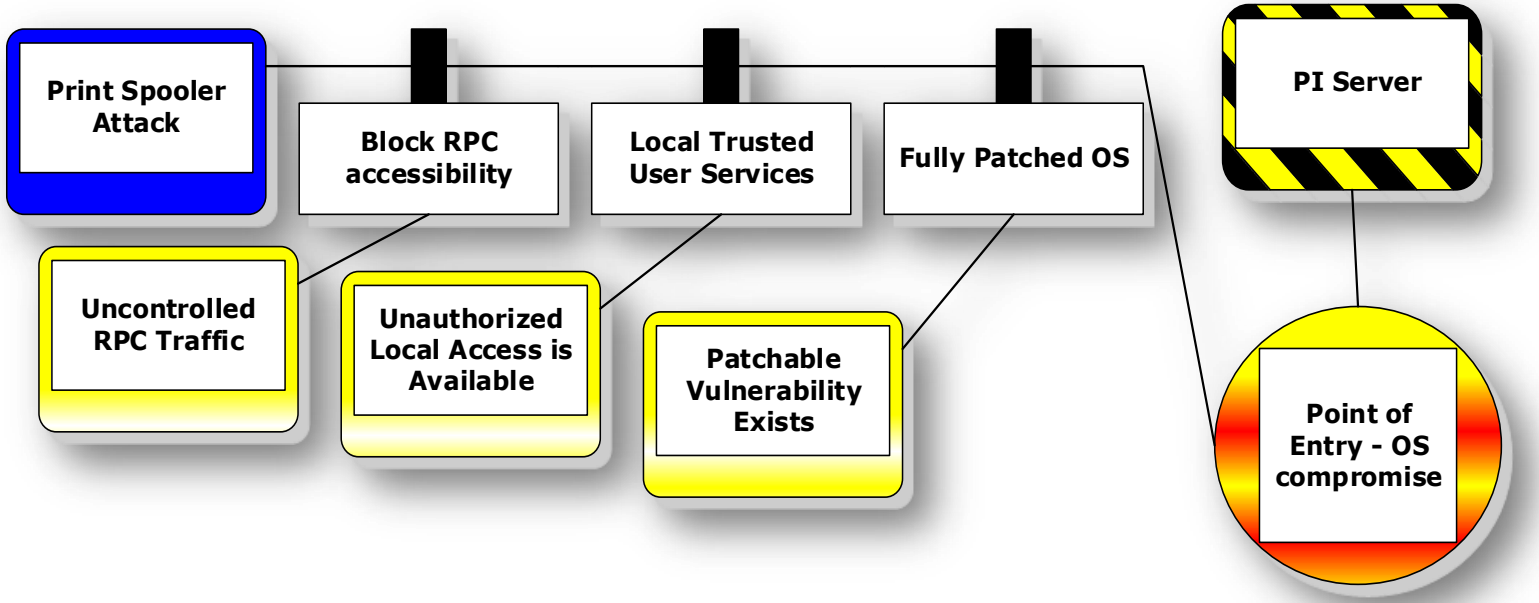
Attacker's Trifecta

Affect 1 factor. Mitigate risk.

- Attackers must have:
  - Vulnerability or config weakness
  - Network comms path
  - Exploit specific to both
- Print spooler 0-day used in Stuxnet
  - Windows OS
  - RPC comms
  - 0-day exploit code

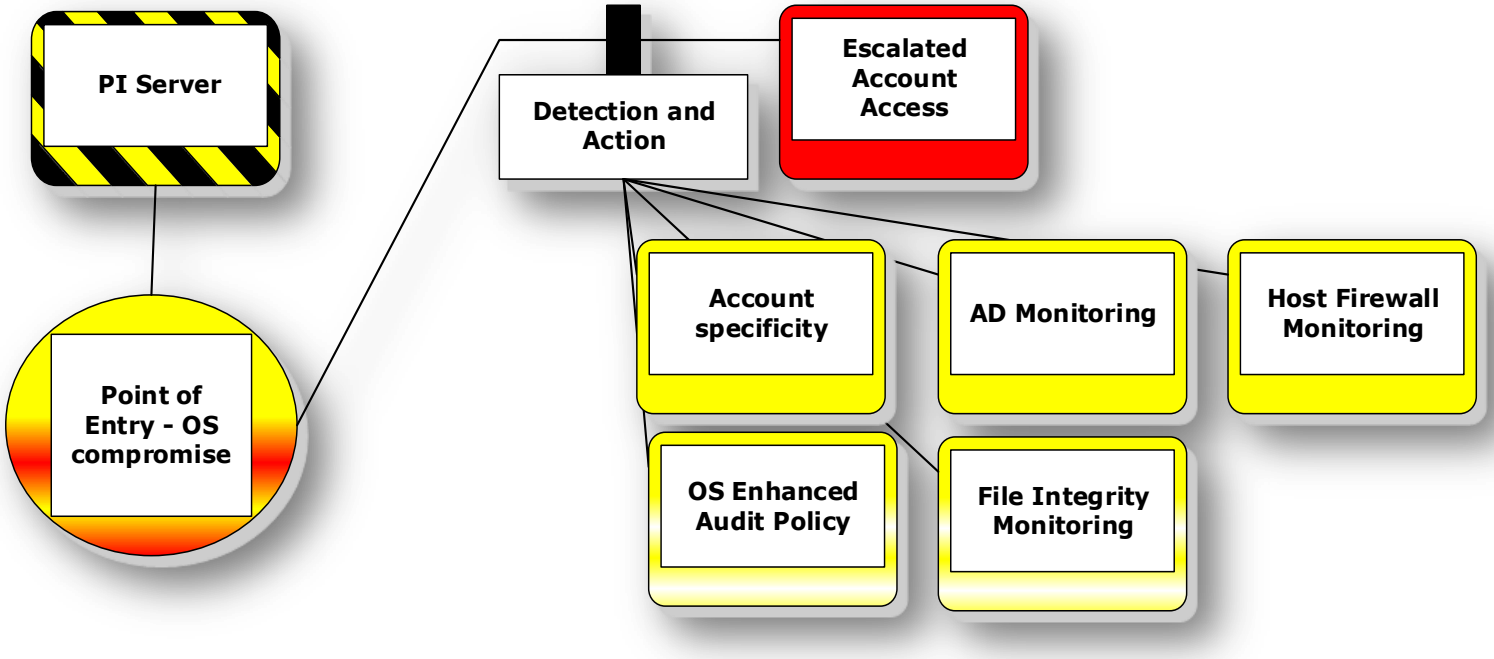
ATAC + Bow Tie Analysis

Why the 0-day worked



ATAC + Bow Tie Analysis

What could have been done



Contact Information

If you need to catch me after you're fully caffeinated…..

Bri Rolston

Chief Research Geek

GkJuju Security Consulting

gkjuju@gmail.com

Questions

Please wait for the **microphone** before asking your questions

State your **name & company**

Please remember to…

Complete the Online Survey for this session

http://ddut.ch/osisoft

감사합니다

谢谢

Danke

Gracias

Merci

Thank You

ありがとう

Спасибо

Obrigado

If questions = 0 Then presentation = fail End If

OSIsoft®

USERS CONFERENCE 2016

April 4-8, 2016 | San Francisco

TRANSFORM YOUR WORLD