

RSA® Conference 2018

San Francisco | April 16–20 | Moscone Center

SESSION ID: HT-T10

HACKING CLOSED NETWORKS

Ira Winkler, CISSP

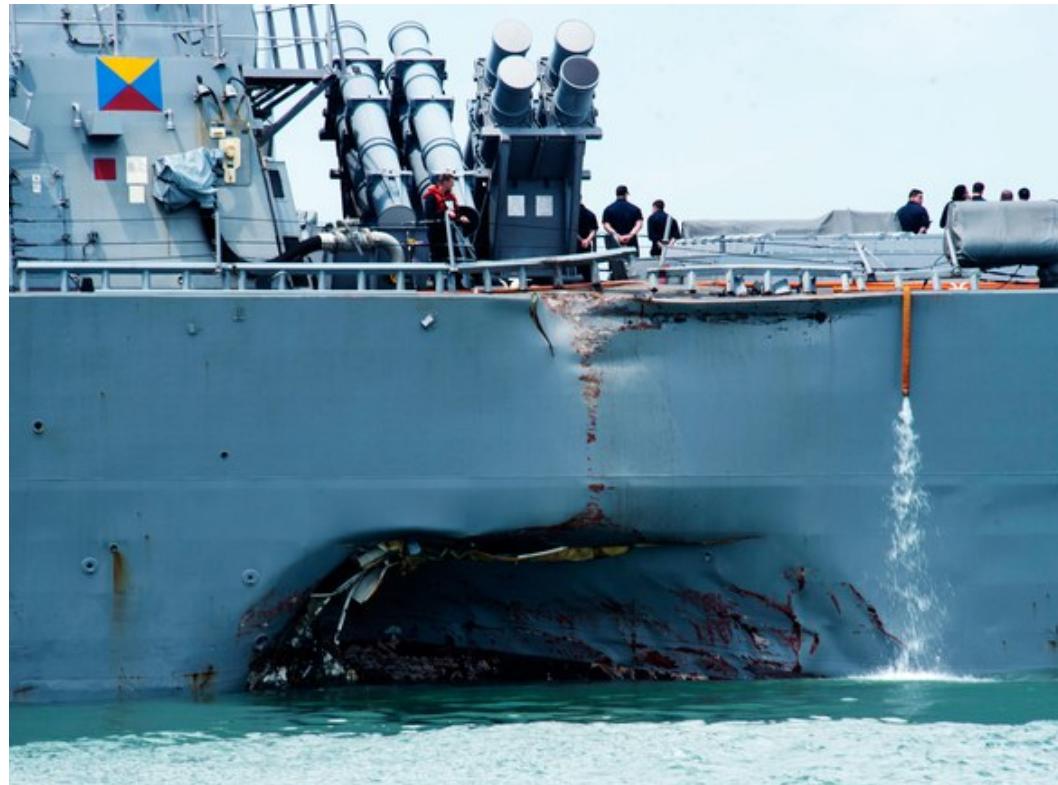
President, Secure Mentem
Advisor, Cylance
@irawinkler



Impossible to Hack



- The network is closed
- It's just a bunch of hype



CYLANCE



**WHAT
ME WORRY?
MAD**

Ignorance is Dangerous, NOT Bliss



- When you don't realize something is a threat, you don't protect against it
- The risk profile must be well understood
- Generally networks are closed, because of the perceived risk

If it's valuable enough to close a network, with all of the costs, it's valuable enough for an attacker to try to find a way in



They Will Fight and Lie to Hide the Vulnerability



Home > Networking

Experts hack power grid in no time

Basic social engineering and browser exploits expose electric production and distribution network



- 2008 RSA presentation about hacking the power grid
- 5 federal agents contacted me
 - 2 unannounced
- Lobbying group said they wanted to talk
 - “It’s not like we want to discredit you, or anything like that”
- Brian Krebs called saying the NRC wanted to brief him on why what I described was impossible
-  ● So he knew I was right



Two Months Later

washingtonpost.com > Technology

TVA Power Plants Vulnerable to Cyber Attacks, GAO Finds

By Brian Krebs

washingtonpost.com Staff Writer

Wednesday, May 21, 2008; 12:01 AM



CYANCE

RSA Conference 2018

The Ways Are Almost Infinite



- Limited by creativity
- Many versions of the different scenarios
- Networks aren't really “closed”
- Access points uncontrolled
- Diagnostic equipment
- Insider abuse
- Compromise developers



Targeting “Closed” Networks



- CERT TA18-074A
 - Russia targeting ICS through multi-stage campaigns
- Watering Hole Attacks
- Phishing
 - Credentials
 - Malware
- Open source information



CYLANCE

RSA Conference 2018

Closed Networks Usually Aren't



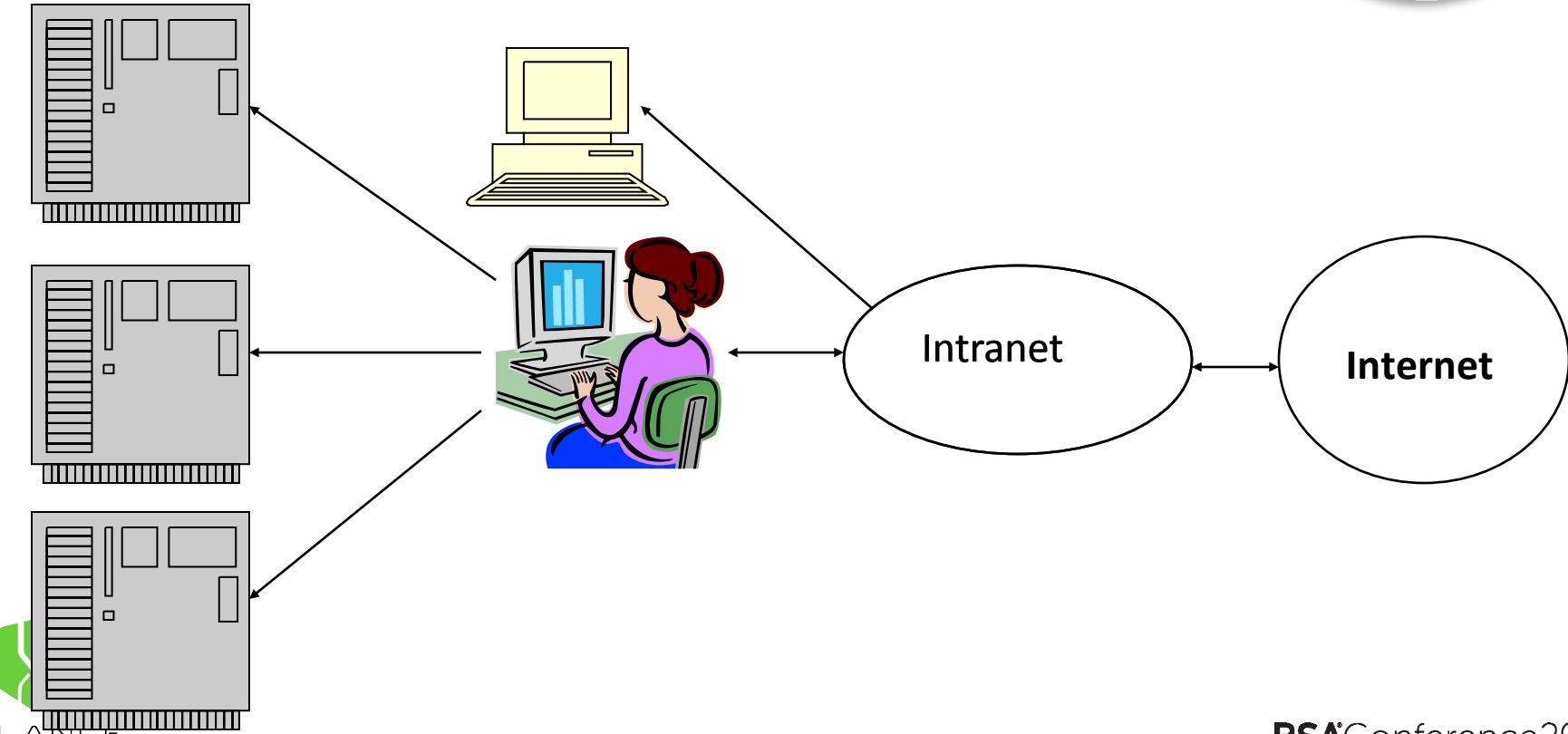
- Might have started out closed
- Functionality added periodically
- Don't want expense of multiple networks
- Put in "limited" connections that really aren't
- Bridges are added



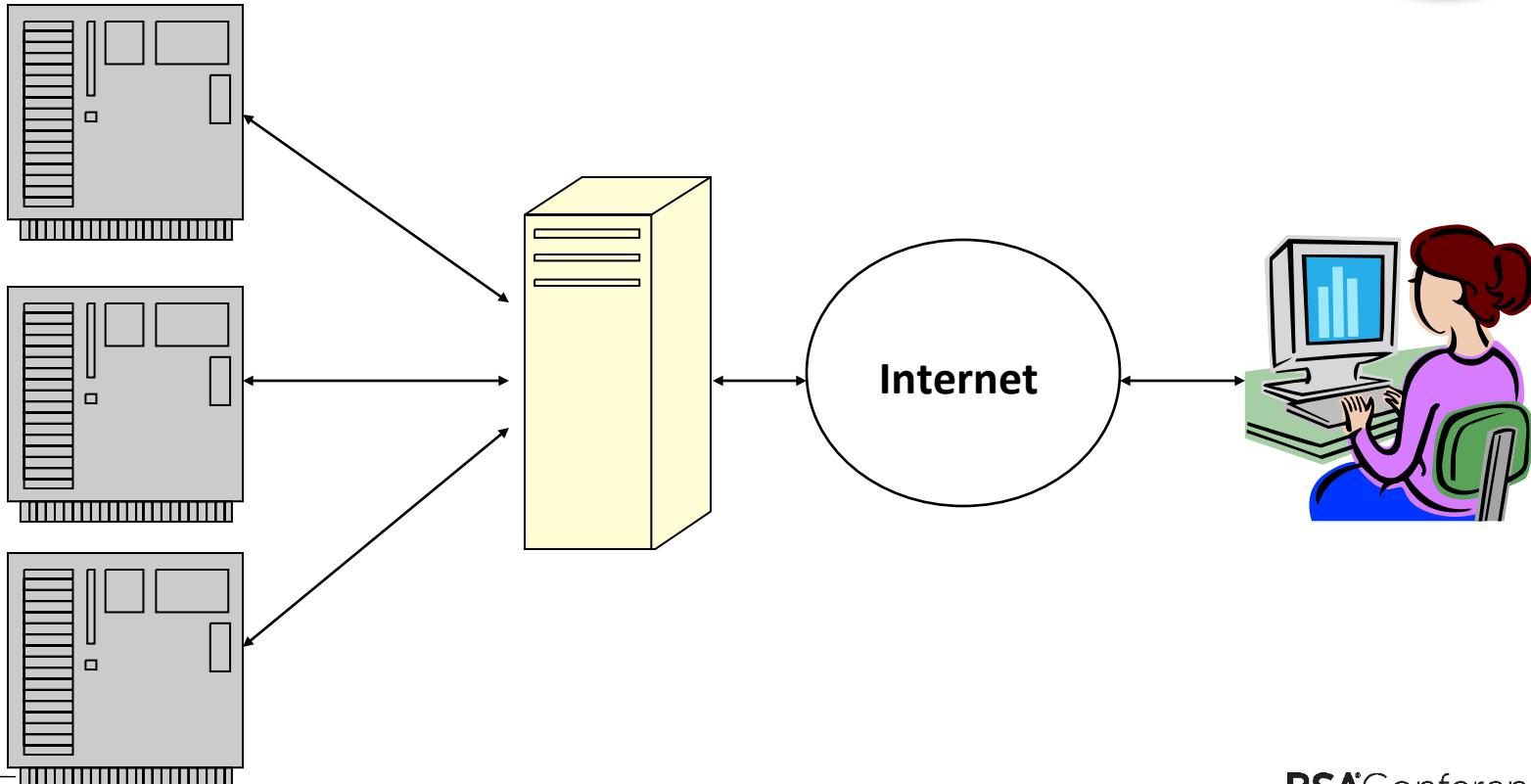
CYANCE

RSA Conference 2018

The Migration



One Example: Power Capacity Sales



Even Worse



- Doesn't include:
 - Wireless
 - Rogue IT
 - Subcontract connections
 - Etc.



CYANCE

RSA Conference 2018

Once In



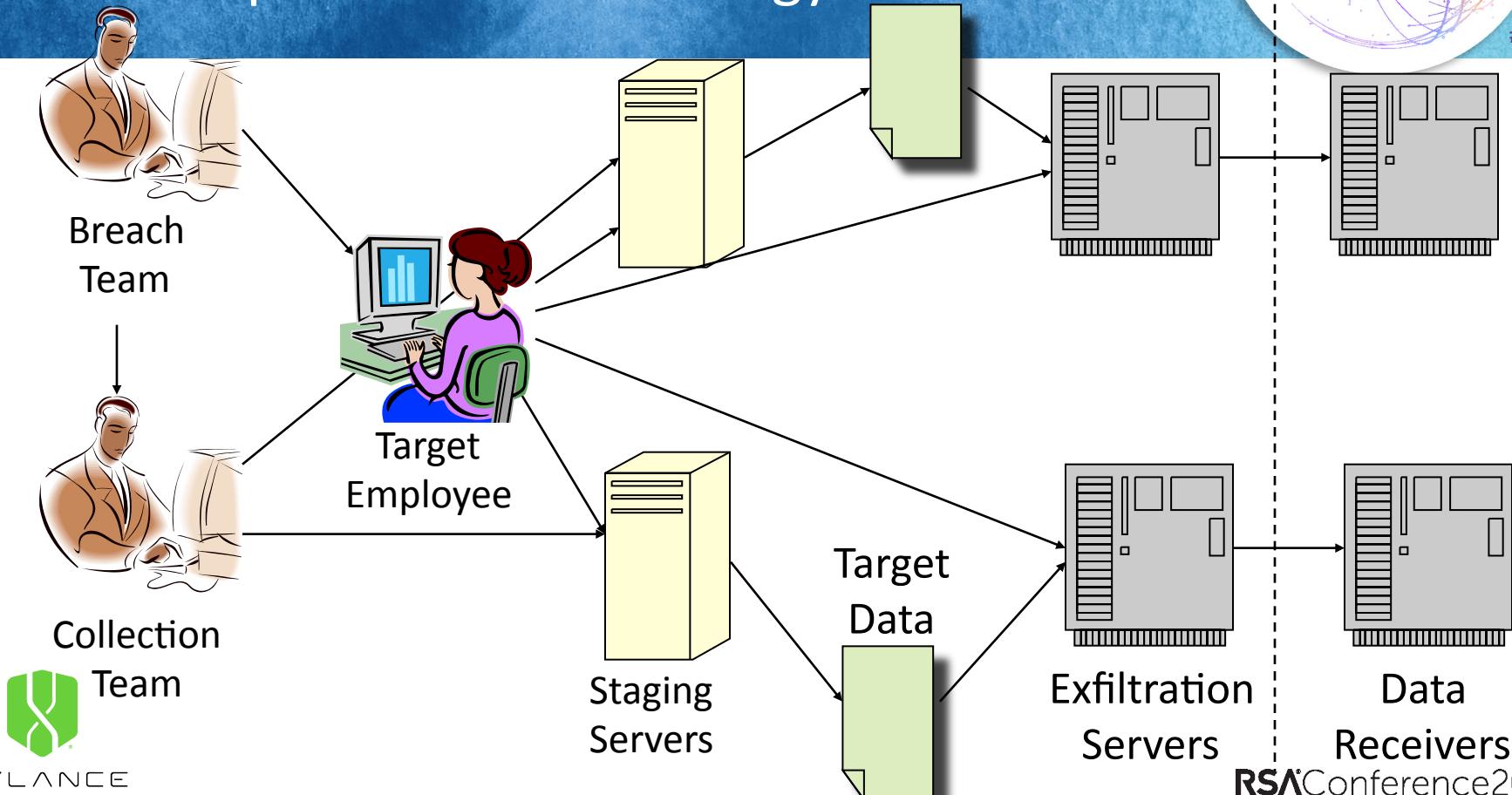
- Systems are frequently not patched
 - WannaCry for example
- Outdated systems
- Insecure configurations



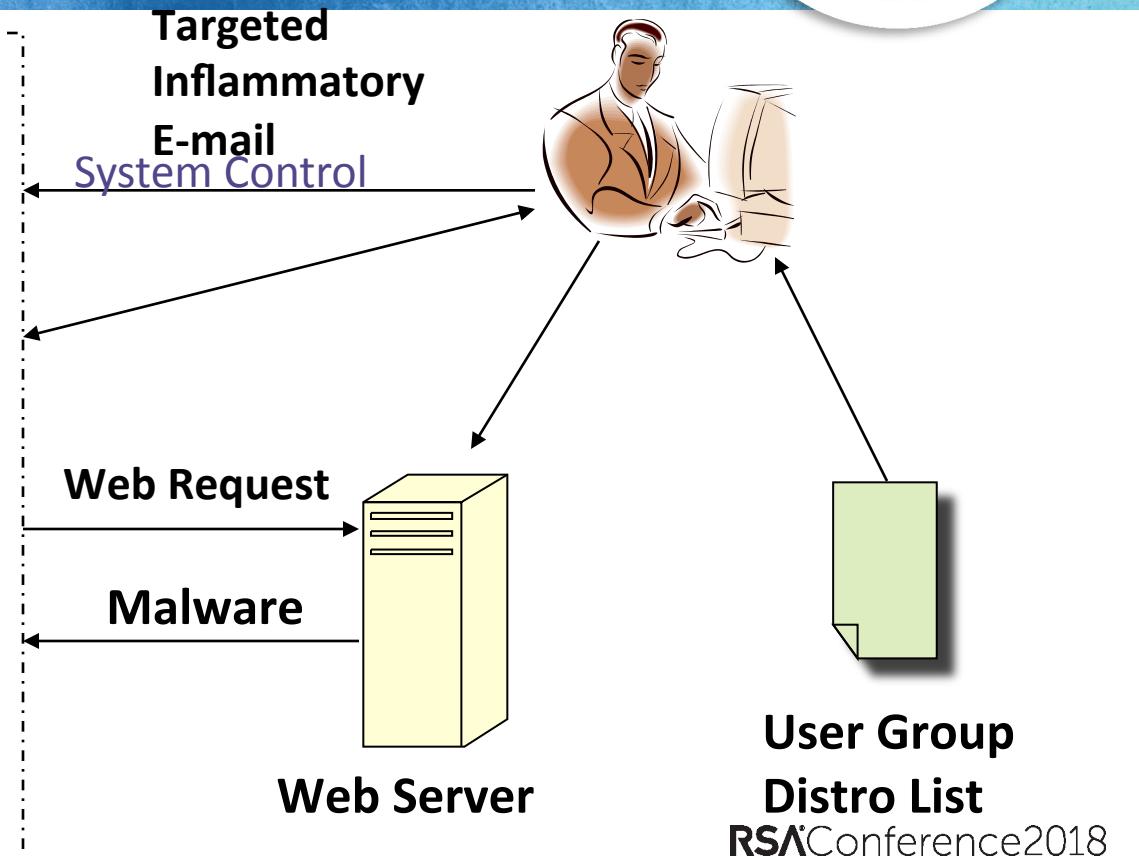
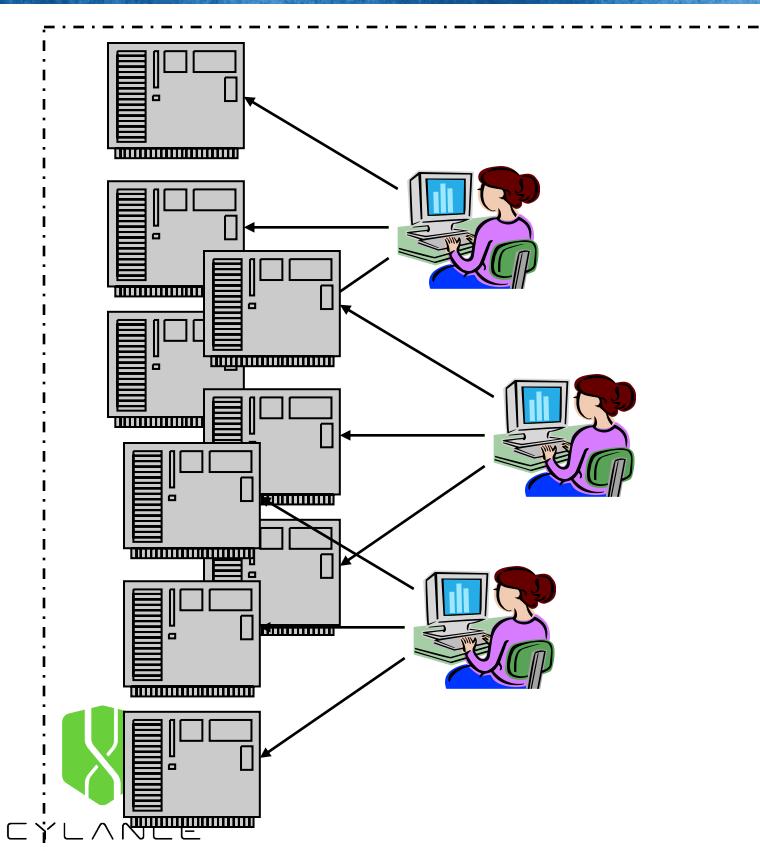
CYANCE

RSA Conference 2018

APT Compromise Methodology



Power Grid Example



General Note



- My case study in 2008
- Siobhon Gorman reported Russia and China hacking US power grid in 2009
- Wired reported it as new on September 6, 2017
- New round of stories on March 15, 2018
- New round of stories in another 6 months
- BTW: Russia hacked Ukraine power grid in June 2017





Uncontrolled Access Points

- Closed networks frequently have many access points
- Power grid has many points where diagnostic equipment can plug in
- Critical infrastructures are distributed and have many access points
 - Consider the Air Traffic Control System – radar, transmitters, airport operations, etc.
 - Water systems have controls throughout hundreds of miles
 - Telecom systems have access points all over



Maroochy Incident



- Vitek Boden worked for a contractor that installed radio controlled SCADA equipment
- Left under bad circumstances
- Stole radio equipment and drove around finding open access points to sewage system
- Released hundred of thousands of gallons of sewage



Diagnostic Equipment



- Can be specialized equipment
- Can be a PC
- Can be a USB device to put in updates
- Plugged into critical systems to perform diagnostics
- Connected to equipment through USB or other connectors



CYLANCE

RSA Conference 2018



Worldwide Issue

- With naval vessels, they can be at all ports around the world
- Think about the thousands of people who have access to a naval base
 - Local contractors
 - Naval personnel
 - Defense contractors
- Not everyone is cleared
- Diagnostic equipment may not be treated as sensitive



CYLANCE

RSA Conference 2018

Some Hacks Require Detailed Research



- Might need to know system configuration
 - Such as Stuxnet
- Might require hacking of contractors development facilities
- Might get from insiders
- Might get from documents available to maintenance personnel or elsewhere
- Some information might be available from open sources



CYLANCE

RSA Conference 2018

Hacking the Developers



- With naval vessels, I mean defense contractors
 - Su Bin group hacked 50 TB from 2008-2014
 - Included details of onboard computer systems
 - BAE Systems hacked in 2009
 - Lockheed Martin hacked in 2011
 - Australian contractor reported hacked in 2017
 - F-35, C-130, and P-8 data hacked, along with 30GB of data about smart bombs and naval vessels
- If you can hack it out, you can put it in



Compromise the Supply Chain



- Intercept equipment to plant malware/proactively sabotage recipient
- Equation Group supposedly doing it since early 2000s
- China accused of doing this
- Stuxnet likely delivered via equipment compromised prior to delivery



Insiders

- Many potential insiders
- Insiders at developers
- Insiders on ships
- Insiders at repair facilities
- Insiders have planted time bombs and sabotaged operations elsewhere
- They've taken things out; little stops them from putting things in



Black Bag Operations



- Outsiders infiltrate an organization
- Can be through pretexts
- Assumed identities
- Get jobs inside targeted organizations
 - Frequently through contractors
- When you don't have or trust insiders
 - Usually a last resort



CYANCE

RSA Conference 2018

Making Closed Networks Open

- A simple patch cable between network equipment
 - If equipment is co-located
 - Ships at sea now provide Internet for morale and other purposes
- Attaching routers to the network
 - Wireless or connected to a cellular/satellite device
 - A more permanent Maroochy
 - There are tools that look for rogue WiFi, so don't laugh
- Modems
 - Yes they still exist





Stuxnet Basics

- In theory, US and Israeli assets determined internal architecture
- Identified software in use
- Developed hack
- Created malware laden USB drives, or
- Compromised supply chain and delivered pre-infected equipment to contractor
- Dropped or delivered drives near developers
- Malware worked autonomously as designed



So, Can You Hack a Naval Vessel?

- Yep, but admittedly complicated
- Stuxnet-like attack strategy
 - Probably autonomous attack
- Determine architecture
- Determine attack vectors
- Plant malware through supply chain, maintenance, or hacking
- Or, placing taps or inside sabotage



CYANCE

RSA Conference 2018



Disclaimer

- Of course, this attack is theoretical
- Similar attacks have been accomplished
- It is more complicated than described, but still possible
 - If anyone said you're going to regularly get malware in an underground Iranian facility, they would have been derided, probably like I will be
- To my terrorist followers, there's not enough here to launch the attacks



Hacking Open Networks Can Use Similar Techniques



- Supply chain, insiders, outsiders, network taps, etc. are still similar threats
- The attack vectors are the same, with a wider attack surface



CYANCE

RSA Conference 2018

Stopping These Things



- Ignorance of the risk is the greatest threat
- Acknowledge the threat
 - Again, if it is valuable enough to cause the network to be closed, it is valuable enough for an outsider to target you
 - Everything is on the table
- Supply chain security
- Protection needs to be as tight as the most valuable open network
- Detection needs to be constant and pervasive
 - Assume technical and physical compromise



CYANCE

RSA Conference 2018

The Big Takeaway



- This can be done
- This has been done
- Saying such an attack is impossible is the greatest threat



CYANCE

RSA Conference 2018

“Apply” Slide



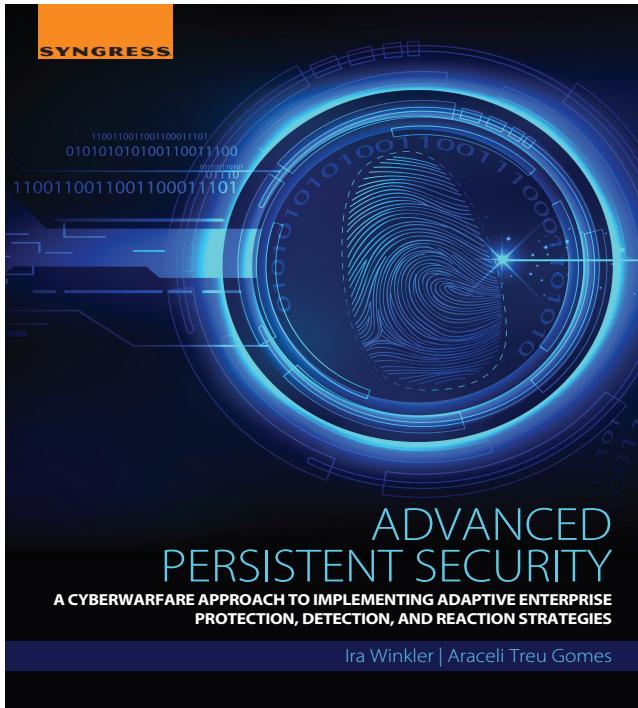
- Within 1 week
 - Determine if you have closed networks
 - Determine if they are actually closed
 - Decide if certain precautions were not taken, because the network is closed
 - Are immediate actions required?
- Within 3 months
 - Plan an assessment/pentest for the closed networks
- Within 6 months
 - Perform the assessment
 - Remediate what you can
 - Plan to remediate
- Actually, the same for Open Networks



The Book, The Myth, The Legend



- Book signing on Thursday



CYLANCE

RSA Conference 2018

For More Information



ira@securementem.com

[@irawinkler](https://twitter.com/irawinkler)

www.securementem.com

www.linkedin.com/in/irawinkler

Facebook.com/irawinkler



CYANCE

RSA Conference 2018