BPM

IT Assurance Across Boundaries

ISC² East Bay Chapter

May 14, 2020

Fast Facts

- *Assessment-Only* Information Security Vendor
  - Singular expertise
  - Objective assessments
  - Cost-effective remediation recommendations
- Providing InfoSec Assessment Services Since 1998
  - Thousands of penetration tests
  - Blackbox & graybox testing activities have often crossed system boundaries, both intentionally and unintentionally
- BPM Infosec assessment team ***are not*** experts at planning, building, or managing infosec controls
  - BPM Infosec assessment ***are*** experts at defeating information security controls and providing infosec controls assurance
  - Thus, this presentation will provide a white hat hacker's perspective on assurance across boundaries

David Trepp
Partner, Information Security Assessment

- US Army Veteran
- MS Geochemistry
- Serial Tech Entrepreneur
- Personal Interests
  - Rock Climbing
  - Bicycle Touring
  - Information Science
    - Thermodynamics

dtrepp@bpmcpa.com

Josh Schmidt
Supervisor, Information Security Assessment

Images Intentionally Deleted

- Senior penetration tester
  - Five years professional penetration testing
  - Ten years system administration
- Answer Driven
  - Pursuit of the “why”
- University of Oregon
- Personal Interests
  - Compression ignition engines
  - Rugby
  - Advanced landscaping

Contents

- The Challenge
- Examples of Breaches Across Boundaries
- Providing Assurance Across System Boundaries

Questions/comments are encouraged

Please do not record images of slides marked Confidential

The Challenge

What Are Your System Boundaries?

Typical Information Systems Have Various Levels of Connectivity with Numerous "Integrated Entities"

- Internal Departments & Devices
  - HR, Finance, Ops, etc.
  - Shadow IT
  - BYOD
  - IoT
- Internal (Segmented) Subnets
  - DMZs
  - Industrial Control Systems/SCADA
  - Cardholder Data Environment (CDE)
  - WiFi Networks
  - Remote Branches/Offices/Employees
- Vendors
  - Product/Application Vendors
  - Support Vendors
  - Hosting/Cloud Vendors
- Government/Industry Agencies
  - Reporting
  - Data Sharing Consortiums
    - Councils of Government
    - Emergency Response Groups

What Are Your Application Boundaries?

Images Intentionally Deleted

Diagram & list of an online banking application's API, batch, and SSO interfaces

How Can One Provide Assurances Across Boundaries?

- You Manage Security for Complex, Interconnected Systems Involving Numerous Integrated Entities
- You Often Don't Have Authority Over Interconnected Systems
  - But you still may be saddled with security responsibility
  - Whether or not you have authority and/or responsibility, the security of integrated entities impacts your system security
- Testing/Assurance Activities with Integrated Entities Are a Microcosm of Overall Governance Challenges
  - Configuration Management
  - Patching/Updating
  - Business Continuity/Disaster Recovery
  - Incident Response
  - Etc.
- We Don't Presume to Have All the Answers to This Dilemma

Not All Entities Have the Same Infosec Priorities

- Traditionally, IT Security Considers Risk to:
  - Confidentiality
  - Integrity
  - Availability

- Security may prioritize Confidentiality
- IT may prioritize Availability
- Application vendors may prioritize Integrity
- Cloud/Hosting providers may prioritize Availability

- Finance may prioritize Cost
- Facilities/Production may prioritize Safety
- Marketing/Business Development may prioritize Ease of Use

Integrated Entities Have Different Infosec Assurance Standards/Requirements

- GLBA
  - Financial institutions
- PCI
  - Payment cards
- HIPAA
  - Healthcare
  - Employee cafeteria plans
- FTC
  - Consumer loans, financing, etc.
- SEC/FINRA
  - Publicly traded companies
  - Brokers-dealers, investment advisors, etc.
- ISO 2700x
  - International standard
- NIST SP 800-171
  - Organizations that do work for certain Federal agencies
- GDPR
  - EU Passport Holders
- CA Privacy & Breach Acts, 23 NYCRR 500, etc.

Integrated Entities May Oppose Your Plans For Assurance Activities

- Organizational, Contractual, or Statutory Prohibitions
- Budget/Human Resource Limits
- Competing Priorities
- Territorialism
- Default Response is “No”
- Fear of Exposure
- Fear of Operational Disruption
- Fear Assurance Vendor Lacks System Specialization

Examples of Breaches Across Boundaries

Internal Boundaries: Network Segmentation

I.

A bank subnet for ATMs is accessible from the administrative network

Images Intentionally Deleted

II.

Network traffic is intercepted

Internal Boundaries: User Privilege Levels

I.

The account appears to have very basic permissions

II.

Images Intentionally Deleted

III.

Despite basic permissions, the account has considerable access

IV.

The low-privilege account is used to access PII and database backups

Internal Boundaries: Outbound Information Flow Control

I.

An outbound DNS query is resolved against a malicious authoritative DNS server

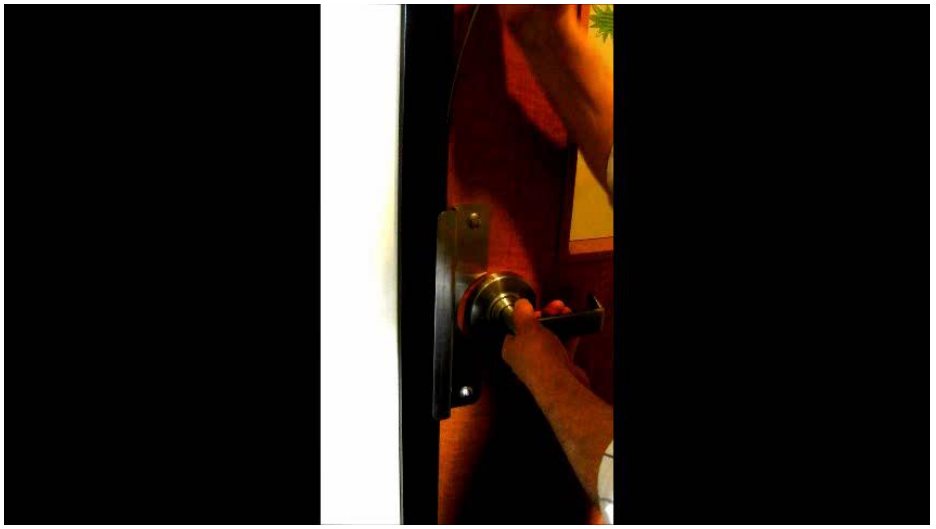
Images Intentionally Deleted

II.

The outbound DNS queries are pre-pended with mock PII - the authoritative DNS server receives the data

Physical Boundaries: Common Weaknesses

Typical double doors



Misaligned anti-shim pin

Portable RFID badge reader

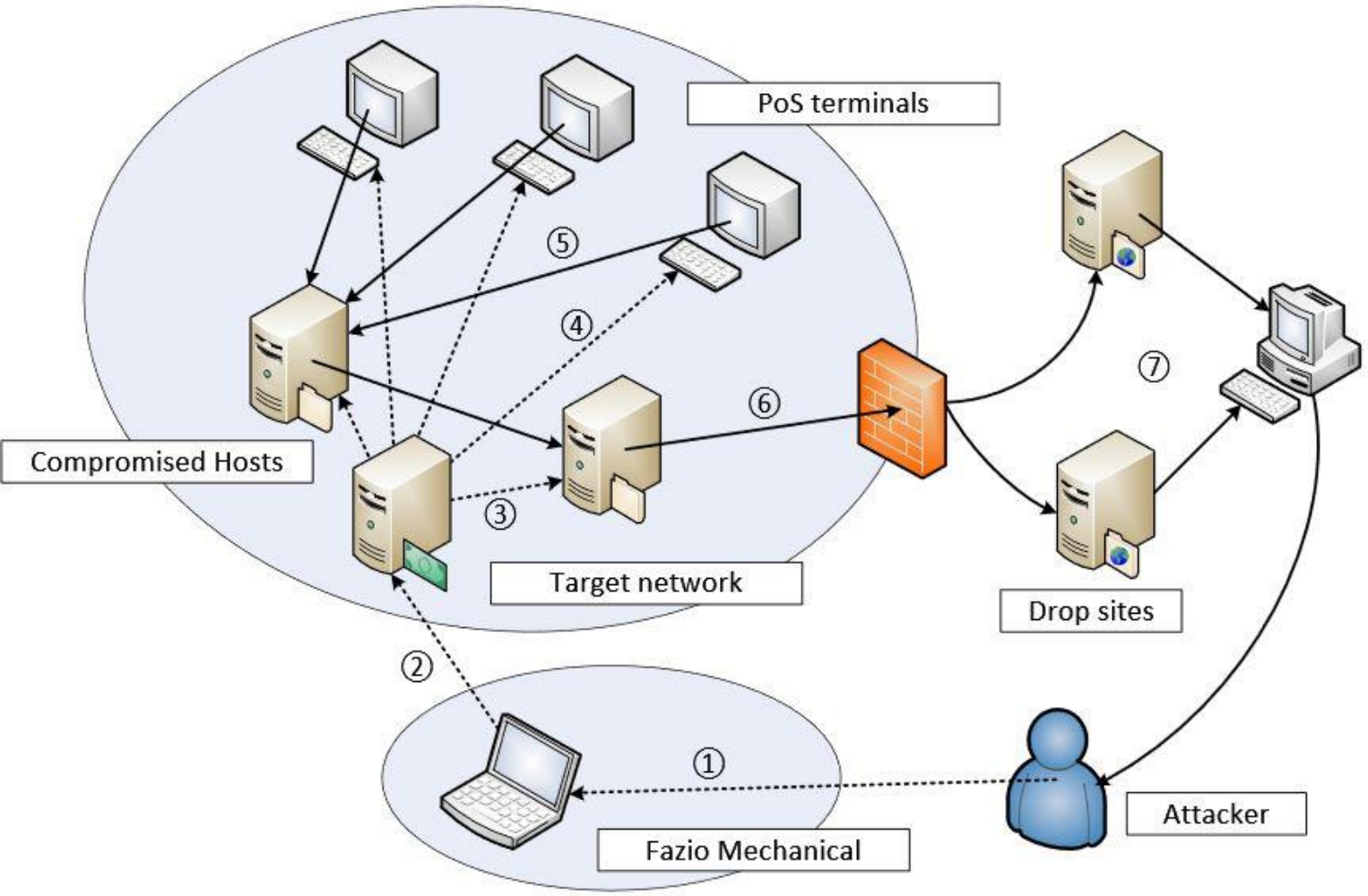
Universal keys

Portable mousejack attack kit

Integrated Entity Archetype: Target Breach 2013

- HVAC Vendor Identified & Breached
  - Via Phish
- Target Provided Remote Access For Vendors
  - Billing, Contract Submission, and Project Management
- Alleged Attack Steps (After Compromising HVAC Vendor)
  - Exploit vulnerable (unpatched) php instance in vendor web app “document upload” feature and establish local host admin
  - Pull NTLM password hashes from LSASS
  - Exploit “pass-the-hash” for DA account privileges
  - Use DA privileges to ransack PoS systems & steal 40 million credit cards
  - Deliver them across the Internet to criminal hosts via DNS exfiltration
- Target Network Lacked Sufficient Controls
  - No multi-factor authentication
  - Inadequate patch management
  - Inadequate vendor server segmentation
  - No Cardholder Data Environment (CDE) segmentation
  - No SMB (digital) signing controls
  - Inadequate information flow controls, specifically network egress controls

Target Breach, continued



Source: **Breaking the Target: An Analysis of Target Data Breach and Lessons Learned**
https://arxiv.org/pdf/1701.04940.pdf

History Repeats Itself: Huddle House Restaurants

"Criminals compromised a *third-party* point of sale vendor's data system and utilized the vendor's assistance tools to gain remote access-and the ability to deploy malware-to some Huddle House corporate and franchisee POS systems."

Source: **https://www.huddlehouse.com/data-protection-notification/**

As viewed February 6, 2019

External Boundaries: Integrated Entity Domain Trusts Relationships

I.

Peer-based name resolution is abused to compel hosts to communicate with the assessment workstation invoking an HTTP authentication prompt

II.

The HTTP authentication attempt is relayed to the domain controller crossing over to LDAPS

III.

Images Intentionally Deleted

LDAP commands are issued using the relayed authenticated session to the domain controller, obtaining a list of all users, groups, computers, trusts, and policies

IV.

Domain trusts reveal a transitive, bi-directional trust relationship with a vendor that also supports other organizations

External Boundaries: Integrated Entity Network Segmentation

I.

Passive network capture is performed

II.

Images Intentionally Deleted

III.

One system is inundating the network with more than 30 packets per second of UDP multicast traffic

IV.

A network mapping tool identified several subnets sending extraneous packets across the network

Hundreds of hosts are identified on the unknown network(s)

V.

Foreign hosts are reachable from the client network

Application Boundaries: Integrated Entity Fails to Validate Account Values

I.

Bank statements are loaded for authenticated user Daisy Duck

II.

Images Intentionally Deleted

A search is initiated

III.

After sending the POST, the server responds with an iframe for an external service

IV.

A second user, Donald Duck, logs in and initiates a search

V

Donald Duck's account value is replaced with Daisy Duck's account value

VI.

Daisy Duck's account statements are now viewed from the Donald Duck account

External Boundaries: Integrated Entity Consortium

I.

II.

Images Intentionally Deleted

A SQL injection vulnerability in the application results in deeper access (excerpt of all database tables)

The Decision Support Collaboration Portal is breached via an automated, lockout-avoiding password guessing attack; access to the Emergency Operations Center (EOC) is achieved

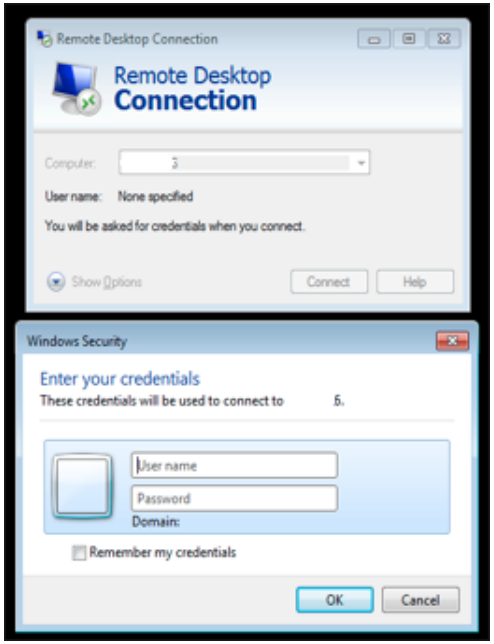
Providing Assurance Across System Boundaries

Define & Document Boundaries

- Inventory & Classify Data Assets
- Inventory & Classify Data
  - At Rest
  - In Transit
- Define Who Is Responsible
  - Ownership
  - Management
  - Security
  - Vendors/contractors/etc.
- Define Boundary Tools & Techniques
  - Firewalls/WAFs/Proxies/Web Filters/etc.
  - VLANs/Subnets/SDNs
  - ACLs
  - AD Group Policies & SSO
  - AD Trust Relationships
  - Vendor Access
  - APIs & Batch Processes
  - Contracts

Vendors: Boundary Security Starts Pre-Purchase

- Disclosure of ***All*** System Access Requirements
  - How is remote access for support handled?
  - What ports are listening?
    - Can handshake attempts be limited by source IP address, certificate, MAC address, etc.?
- Disclosure of ***All*** Accounts
  - What are minimum authentication requirements?
  - What are privilege levels?
  - Have all default credentials been changed?
- Disclosure of ***All*** Communications Protocols
  - What internal traffic is expected?
  - What inbound/outbound traffic is expected?
  - How is patching/updating/change management handled?



- Permission to Include Their System within the Scope of Testing Regimen
  - Or Demand Evidence of Their Ongoing Test Regimen

Does The Vendor Exhibit a Culture of Cybersecurity?

Vendor Boundary Controls: Standards & Regulations

A Few Universal Standards

- ISO 27001
  - A.15 Supplier Relationships
    - A.15.1.1 Infosec policy for suppliers relationships
    - A.15.1.2 Addressing Security within Supplier Agreements
    - A.15.2.1 Monitoring and review of supplier services
    - A.15.2.2 Managing changes to supplier services

  1) Suppliers only have access to systems (and data) that they are specifically authorized for
  2) Supplier access is managed, controlled, monitored, and time-bound
  3) Suppliers have a suitable baseline level of security, commensurate with your organization's security posture
  4) Suppliers are governed by security policies and procedures, and subject to non-disclosure and confidentiality clauses
  5) Suppliers are delivering services as anticipated and that any lack of service provision does not adversely affect the organization, or expose the organization to unnecessary risk

- NIST 800-53
  - AC-4: Information Flow Enforcement
  - CA-3: System Interconnections
  - CA-7: Continuous Monitoring
  - SA-9: External Information System Services

- NIST SP 800-47 *Security Guide for Interconnecting Information Technology Systems*

A Few Regulations

- GLBA
  - Oversee service provider arrangements
- PCI
  - Requirements for Shared Hosting Providers
  - Segmentation and sampling
- HIPAA
  - Business Associate Contracts and other arrangements
- GDPR
  - Data protection by design and default

Boundary Controls: Interconnect Security Agreements

- Interconnection Statement of Requirements
  - The requirement for the interconnection, including the benefits derived
  - The names of the systems being interconnected
  - The agency name or organization that initiated the requirement. If the requirement is generated by a higher level agency or organization, indicate the name of the organization and the individual that requested the interconnection, if appropriate
- System Security Considerations
  - General Information/Data Description
  - Services Offered
  - Data Sensitivity
  - User Community
  - Information Exchange Security
  - Rules of Behavior (*include permission to test*)
  - Formal Security Policy for each organization
  - Incident Reporting
  - Audit Trail Responsibilities
  - Security Parameters
  - Operational Security Mode
  - Training and Awareness
  - Specific Equipment Restrictions
  - Dialup and Broadband Connectivity
  - Security Documentation
- Topological Drawing
  - All communications paths, circuits, and other components used for the interconnection
  - Depict the logical location of all components
- Signatory Authority
  - The expiration date of the agreement
  - Periodic review requirements, such as the date of the next review
  - Other statements as required
  - The signatures of authorities from each organization and the date of the signatures

See NIST SP 800-47 *Security Guide for Interconnecting Information Technology Systems*

Integrated Entities: Trust, But Verify

- Comprehensive Penetration Testing
  - Only a comprehensive test can reveal cascading sequences of exploits
  - Carefully define test boundaries
    - The entire network, including physical, social, phone, email, etc.
    - Vendor premise equipment
    - Hosted websites
    - Key cloud applications & systems
    - Etc.
- Boundary & Segmentation Testing
  - DMZ
  - CDE
  - Wireless/guest networks & systems
  - SCADA/ICS
  - VoIP & point-to-point communications systems
- Application Penetration Testing
  - Developer's access
  - Shared hosting
  - Calls to 3rd parties, *e.g.* API's batch process, SSOs, etc.
  - Cypher suites for clients

Integrated Entities: Arguments

- Insist That Assurance Activities Are Necessary for All Integrated Entities
  - To confirm effectiveness of boundary/segmentation controls
  - To meet regulatory guidelines
  - To get an accurate assessment of your security posture
- Don’t Leave Them in the Dark
  - Keep them informed from the start
- Reassure Them
  - The object is not to make them look bad
- Remind Them We’re All In This Together
  - Avoiding breaches avoids scapegoats
- Thank Them for Putting up With the Testing/Assessment
- If Insisting, Reassuring, Thanking, and Begging All Fail…
  - Demand evidence of the integrated entity's active InfoSec risk management program
    - Risk Assessment Plan of Action
    - Penetration test attestation
    - Security Policy and/or Catalog of Controls
    - SOC II, ISO 27001, FedRAMP, and/or other relevant certification

Boundary Controls & Cyber Liability Insurance

- Examine Policy Terms: What Systems Are Covered?
  - Industrial Control, IoT & ATM systems?
  - Mobile devices?
  - Vendor owned/managed systems?
  - Contractor hosts?
  - Cloud systems and applications?
- Are There Exceptions to Coverage Related to Inadequate Due Diligence?
  - Vendor management?
  - Configuration management?
- Examine Policy Terms: What Will the Policy Pay For?
  - Business interruption costs?
  - Reputation loss costs?
  - Legal fees?
  - Regulatory claims & fines?
  - Forensics & recovery costs?
- Examine Policy Terms: What Constitutes a Covered Data Security Breach?
  - Is a social engineering attack covered?
  - Is a ransomware attack covered?
  - Is a physical attack covered?
  - Is an inadvertent PII disclosure covered?
  - Is a state-sponsored act covered?
  - Is a prior act covered?
  - Are losses outside a breach event covered, *e.g.* client-led class-action suit?
- Are there any overlapping provisions with other policies, *e.g.* bus. interruption also covered by property policy?
- Be Brutally Honest Filling Out the Application/Questionnaire
  - Your claim may be denied for a fraudulent application

Physical Boundary Controls

- Effective Ingress Controls, *i.e.* Door Locks
  - Physical
  - Electronic
- Effective Surveillance
- Employee & Visitor Least Privilege
  - Limit vendor access to required areas
  - Strong badge controls
    - Keep badge images off social media
    - Color coding for easy ID
    - Printing on back side
    - Standardized photo's
- Disable Unused Ports
  - Network
  - USB
- Six-Wall Security for Sensitive Data Assets
- Isolate and/or Secure Data Closets/Racks
- Wireless Boundaries
  - RFID Badges
  - HIDs, *e.g.* wireless mice
  - WiFi Enabled Peripherals, *e.g.* printers

Images Intentionally Deleted

Default Cloud Configuration Issues

- Outlook\Exchange
  - EWS & MFA
  - MAPI/Modern Authentication
- Azure AD
  - Examine default access
  - Wade through permission management
- AWS
  - Define user policies
  - Enforce permission boundaries
- Allocating enough time at the admin console
  - AWS Security Hub
  - MS Security Center
- Adequate Log Storage

Information Flow Controls

- Baseline Normal Boundary Traffic
  - Internal, e.g. CDE, DMZ, ATM, etc.
  - External, e.g. Web, VPN, Email, DMZ, Vendor, Customer, etc.

- Implement Controls
  - Firewalls/ACLS
  - 802.1x/Mac-Address Filtering/Dynamic ARP Inspection
  - IDS/IPS/SIEM
  - Email DLP

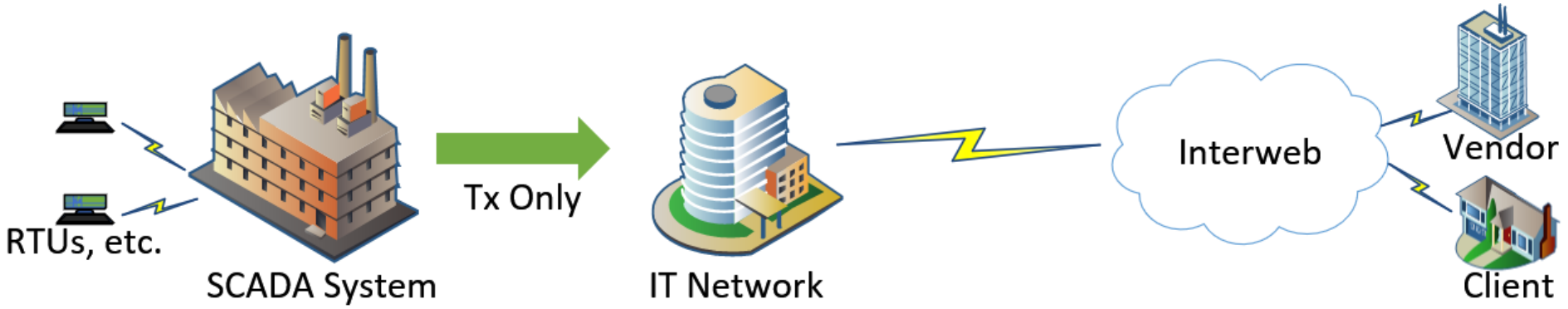
What, exactly, constitutes “secure” remote access?

Information Flow Controls, Cont.

- Lightweight covert channel egress controls
  - Exfiltrating data via FTP over TCP port 80 or 443
    - Web Proxy
    - Whitelisting (Blacklisting is eternally a step behind)
    - Deep packet inspection/DLP
- Heavyweight covert channel egress controls
  - Exfiltrating data prepended to outbound DNS queries & ICMP requests
    - Block outbound ICMP (except maybe 8.8.8.8)
    - Proxy, whitelist, and/or Rate Limit DNS

ICS Information Flow Controls

- Use DHS ICS-CERT CyberSecurity Evaluation Tool (CSET)
  - Baseline ICS security posture
    - With asset inventory from GRASSMARLIN discovery tool
- Removable Media Prohibitions/Restrictions
- Transient/Roaming Device Controls
- Consider Uni-directional OT communications, *i.e.* data diodes
  - Patches/updates via proprietary back door or sneaker-net



Additional Technical Boundary Controls

- Default Configuration Controls
  - Harden default credentials
  - Harden default settings
  - Reduce attack surface area
    - SNMP
    - RDP
    - NTP
    - Vendor remote access
- Least Privilege Controls
  - VPN/webmail/portal
  - Inter-domain trust
  - Visitor/vendor/contractor
  - Typical internal user
  - Elevated privilege internal user
- Promiscuous Protocol Controls
  - LLMNR/NBT-NS
  - WPAD
  - IPv6
  - HTTP, FTP, Telnet, RDP, and other cleartext protocols
- Access & Authentication Controls
  - 2FA, Public Keys, etc.
  - SMB Signing
  - LDAP Signing
- Assurance Controls
  - Test to see if boundary controls function as intended

Vendor default configurations for some common surveillance systems include well-known default passwords

Images Intentionally Deleted

Use Assessors Who Speak Their Language

- Secure Data Handling Practices
  - Segregation & least privilege
  - Encryption
  - Strong authentication
  - Cloud controls/prohibitions
  - Secure data destruction
- Possess Relevant Certifications & Industry Experience
- No Conflict-of-Interest Services
  - Shouldn’t be planning, building, or managing any systems being assessed
- Ready to Work with Integrated Entities
  - Permission procedures & templates
  - Test during non-peak hours & support availability
  - Tailor tests to entity requirements

Conclusions

- Providing assurance across system boundaries is a growing challenge
- The security posture of each integrated entity influences the security posture of all entities
- Even if testing across boundaries of integrated entities is not permitted, addressing the issue will:
  - Increase communication
  - Improve security awareness
  - Inspire action

Recommended Reading

- DHS

Securing High Value Assets
https://www.dhs.gov/sites/default/files/publications/Securing%20High%20Value%20Assets_Version%201.1_July%202018_508c.pdf

- NIST SP 800-47

Security Guide for Interconnecting Information Technology Systems
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-47.pdf

- NIST SP 800-53 Rev4

Security and Privacy Controls for Federal Information Systems and Organizations

AC-4: Information Flow Enforcement
CA-3: System Interconnections
CA-7: Continuous Monitoring
SA-9: External Information System Services

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Questions/Comments?

Thank You!