



## THE FIRST MILE

---

# Client Side Security for Remote Access to Control Systems

Presented by: Mark Zanotti  
Shane Mason

# WHO WE ARE

---

- Lofty Perch
  - Mark Zanotti
    - CTO, VP Engineering
  - Shane Mason
    - Director of Training
- A ICS centric cyber security team
  - The issues and solutions we present here are based on information collected from cyber security research and onsite experience within ICS domains.

# WIDE USE OF REMOTE ACCESS

---

- Control system engineers use remote access for many reasons
  - Emergency access
  - Geographical distance
  - Convenience

# SECURITY ARCHITECTURE

---

- There are several security problems with accessing ICS environments
  - Internet/corporate access allows inbound access  
*Firewalls*
  - Clear text communications can be accessed or hijacked  
*VPNs & Encryption*
  - Allowed inbound services have vulnerabilities which can be exploited  
*IDS/IPS & Application Firewalls*
  - Clients which are allowed to connect have vulnerabilities which can be exploited

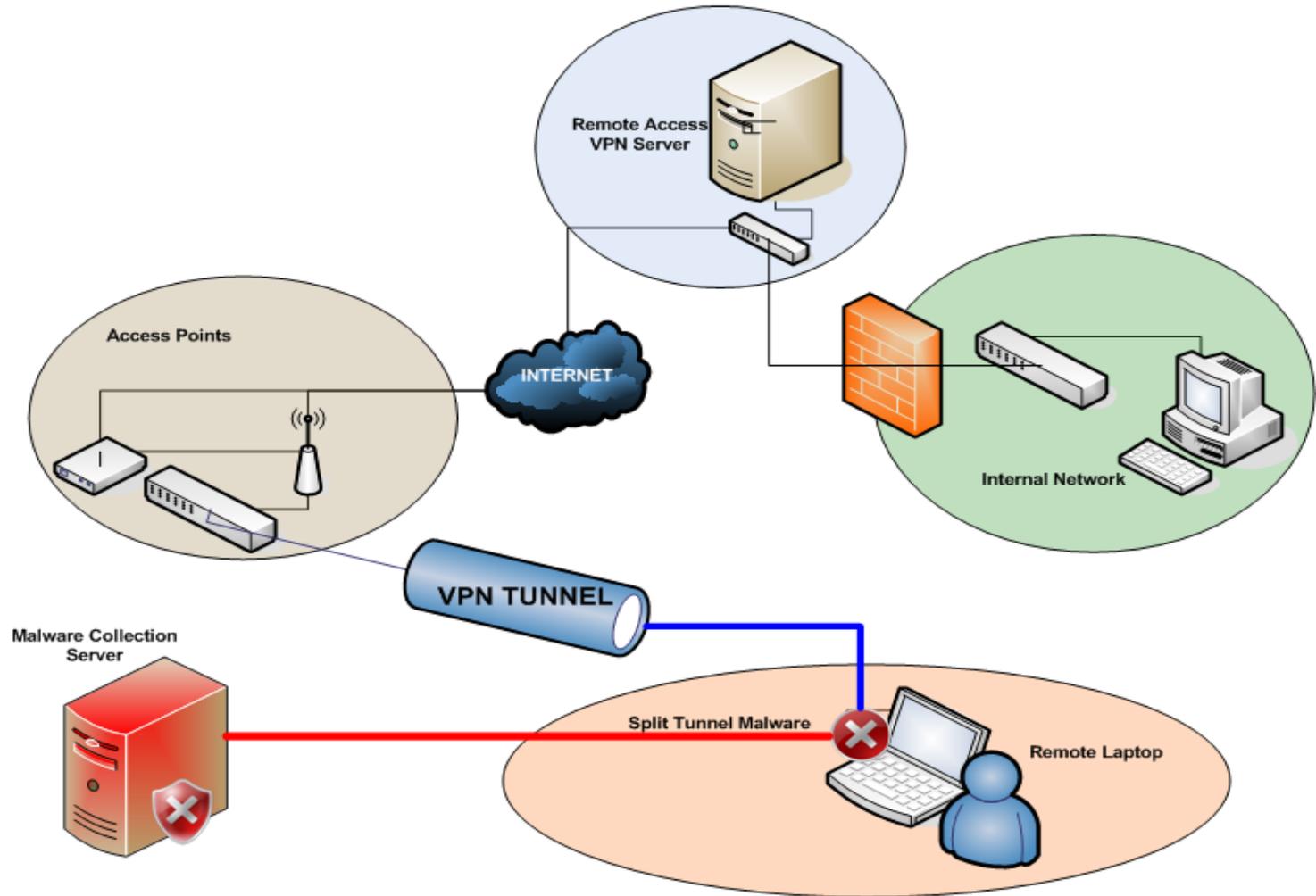
# THREATS – VIRUS INFECTIONS

---

## Emergency access from home

- *The operator has used this corporate system on many public networks, including his/her home network*
- *The corporate laptop is infected with an ICS specific virus*
- *The virus uses the trusted connection established with the ICS to infect systems there*

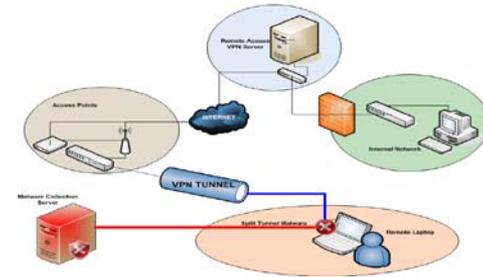
# THREATS – SPLIT TUNNELING EXAMPLE



# THREATS – SPLIT TUNNELING

---

## 1. Split Tunneling



- *The operator system allows network connections simultaneously with VPN connections*
- *While connected to both the ICS environment and the Internet, their laptop is hacked*
- *The attacker has access into the ICS environment*

# THREATS

---

Hey, what are you doing there?



- Piggybacking
  - In each of the previous examples, an attacker “piggybacks” on a valid connection
  - The connection is validated, so the traffic passing through the connection is considered valid
  - IDS/IPS systems have some effect, in that they can detect some anomalous behavior
- Securing the remote client is a high priority

# CLIENT SIDE SECURITY – WHAT HAS GONE BEFORE

---

- How can we KNOW that the client is secure?



- Anti-Virus

- *Gets turned off by administrators because of system performance*
- *Is a reactive technology, and susceptible to Zero-Day attacks*



- System Hardening

- *Undermined by the installation of new software*



- Host Firewalls

- *Are loose to ensure performance and functionality of services*
- *Do not protect against improper activity by a permitted service*



- Host IDS/IPS

- *Are reactive technologies, and susceptible to Zero-Day attacks*

## NEXT STEP – ASSUME CLIENT SYSTEM IS COMPROMISED

---

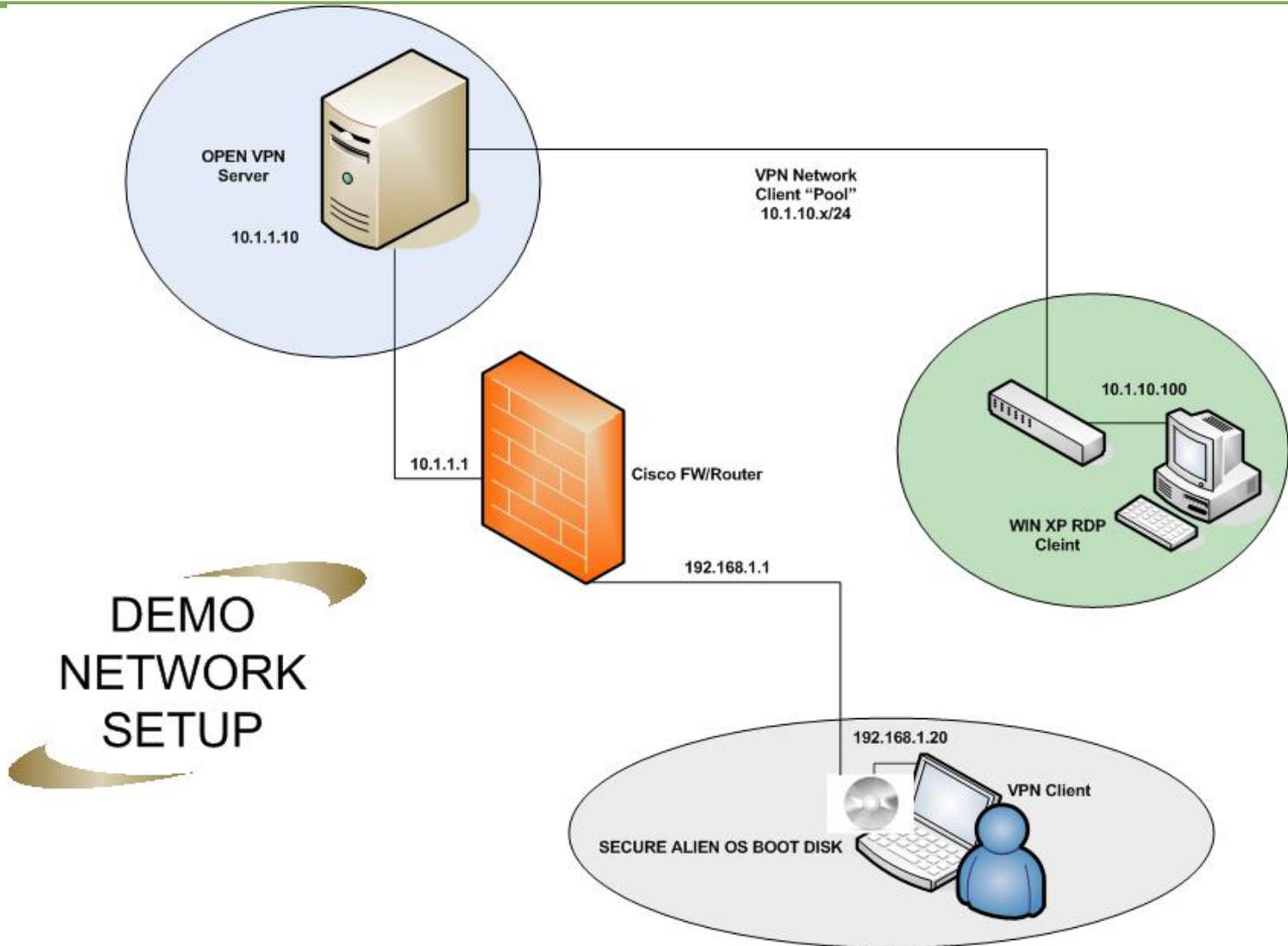
- Assume that the client system is compromised
- Alien OS on CD/DVD
  - Clean boot image
    - *The image is on a known clean DVD or CD*
    - *CDs and DVDs are not writable, so are protected from infection*
  - Different OS than the incumbent
    - *Infections on the host system are incompatible with the running OS*
  - Not a virtual session within the current OS

# THE SOLUTION CONTINUED

---

- Alien OS
  - Linux distribution
    - *Very few viruses are in the wild which affect it*
    - *Easy to harden the image*
  - Minimal, hardened image
    - *As few services as possible, to reduce attack surface*
    - *Firewall included to eliminate inbound access*
  - VPN capability for remote access
    - *Support for high-security communications channels*
  - Remote Desktop and/or Citrix Client
    - *Control the user experience*
    - *Reduce attack surface for inbound attacks from clients*

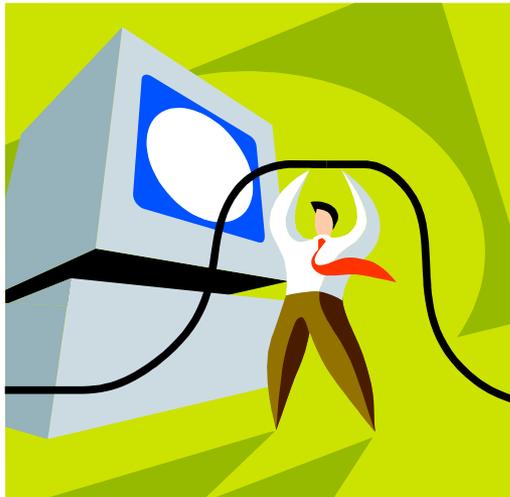
# DEMONSTRATION NETWORK SETUP



DEMO  
NETWORK  
SETUP

# DEMONSTRATION

---



# FUTURE THOUGHTS

---

- **Individual Customization**
  - Strong Authentication
  - Certificates
  - Instant, individualized build process
- **Ease of Use**
  - Graphical interfaces to manage functions must be created
  - Server based functionality for quick re-mastering of CDs/DVDs
- **Convenience**
  - Can we make it so you don't have to exit your current session???
  - Use VMs (vmware, virtual PC, etc)

# CREDITS

---

- Jeffery Douglas Waddell  
([jefferydouglaswaddell@gmail.com](mailto:jefferydouglaswaddell@gmail.com))
  - “Secure Boot Disk VPN”
  - <http://www.ibiblio.org/pub/linux/docs/howto/Secure-BootCD-VPN-HOWTO>
  - Excellent walk through using DSLinux.
- OpenVpn
  - <http://www.OpenVPN.net>
  - Excellent support through forums and community
- Live CD List
  - <http://www.livecdlist.com>
  - Good resource for picking a Distro (last updates, ratings, size)



**THANK YOU**

---

**Questions?**