

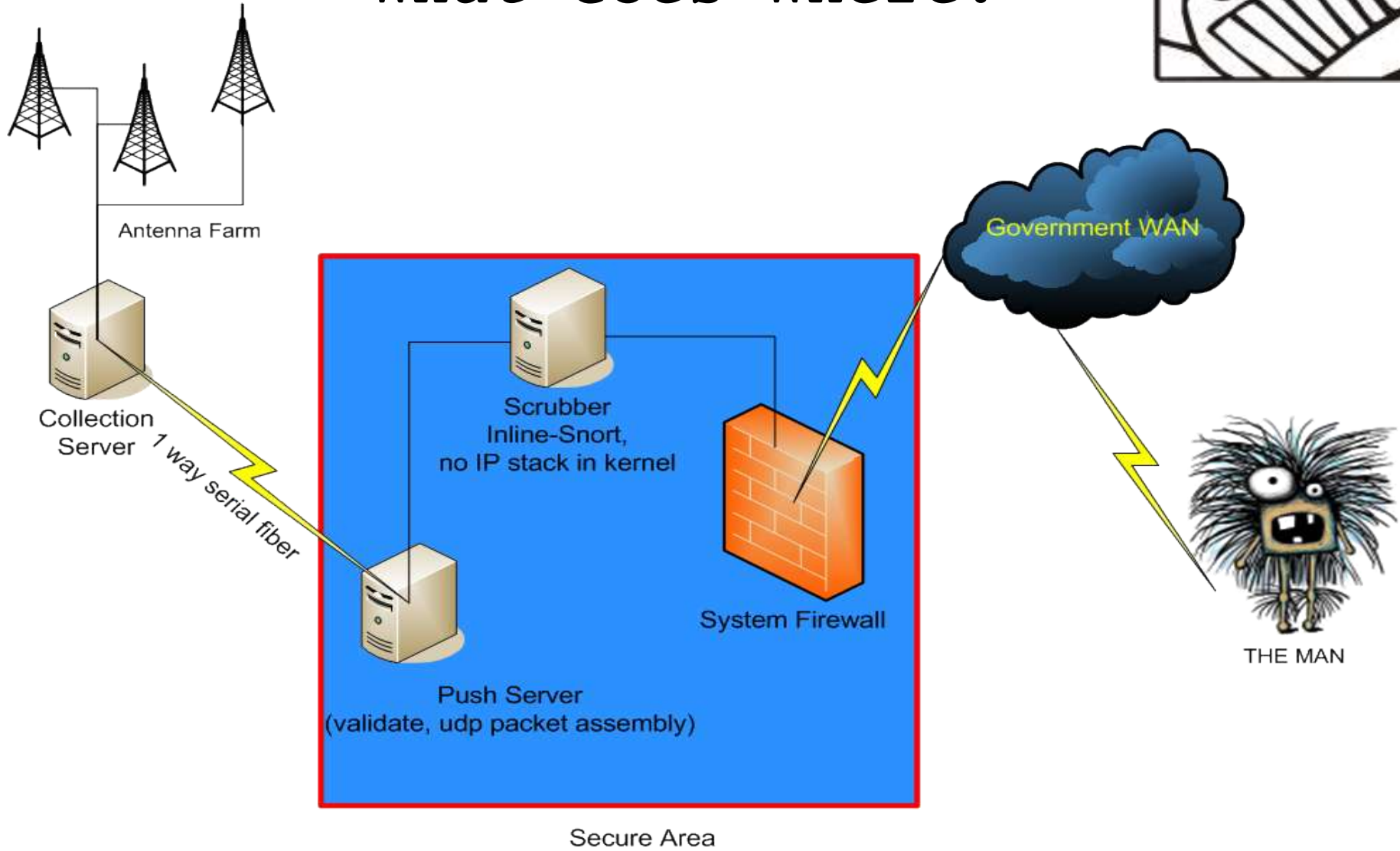
Executive Summary



- Data in the air
 - Snatched by antennas
 - Antennas not protected
 - Antenna Farmers not all spooks
- Data pushed from antennas to Vault
 - Dropped off onto classified network
 - Data cannot come back up from vault
- Data packaged and pushed from vault to The Man
 - The Man wants limited reach into his clubhouse
 - Data becomes classified as it mingles with other packets on the networks

This Space Intentionally Left Blank

What Goes Where?



This Space Intentionally Left Blank

Problem



- Antenna Farm administered by Engineers
 - Not all have a "need-to-know" for each aspect of project
 - Antennas in unsecured location
 - Data collects unclassified
- Collector (Push) system requires *integrity*
 - System is unclassified
 - Must guarantee it has not been tampered with
 - Access to the console requires physical admittance to vault
- Data scrubber requires *integrity*
- Data scrub box is gateway to classified networks
 - Passes acceptable packets onto network through firewall
 - Logs and drops unacceptable packets

This Space Intentionally Left Blank

Requirements



- Collects need to be as *realtime* as possible
- Must ensure that *no* sensitive data taints the unclass portions
 - Antennas, Push/Packaging system, and internal scrub box are all unclassified
 - Once collated with other downstream data, the collects become sensitive by association
- Only data limited to the collects is allowed to enter the government network side
- Did we mention no data driftback is allowed?
 - Government very emphatic on this point
- System must provide extensive test evidence of proper performance before allowed initial run
 - Tedious proof of concept scenarios completed and documented

This Space Intentionally Left Blank

Solve The Issues



- Not all involved cleared for access to highest level of data
 - Keep uncleared and DoD personnel out of the vault
 - Ensure data flows in one direction only
- Ensure no data tainting takes place on UNCLASSIFIED systems
 - One-way fiber link between antennas/collect system and packager
 - Inline_Snort system between push system and classified network
- Ensure integrity of packaging system
 - Only accept data from one MAC address on one interface
 - Limit number of accounts on system
 - Highly regulate and document all configuration changes
- Ensure integrity of packet scrubber
 - No IP stack in the operating kernel

This Space Intentionally Left Blank

Solve The Issues (Cont'd)



- Limit data entering the far-end network to project data only
 - Scrubber ruleset severely limits what passes through
 - Firewall rules further filter what travels to far-end

This Space Intentionally Left Blank

Data Flow Mitigations



- Signal Of Interest intercepted by Antennas
- Antennas' collection system passes the data down to the bespoke data packaging application via one-way fiber transmission
 - Ethernet to Fiber transceivers used with only the receive side connected
 - Beyond this segment of the hardware requires
 - Intel clearances
 - Physical access to the vault
- Package system crafts custom udp packet and passes it along
 - Inserts a numeric code in unused header segment???
 - Ensures data is uncorrupted and packages it for transport
 - Hands packets off to external interface of Inline_Snort system via crossover ethernet cable

This Space Intentionally Left Blank

Data Flow (Continued)



- Packet scrubber decides whether or not to pass data onwards
 - Looks over header for numeric trigger
 - If trigger present data is passed out the other interface
 - If trigger not present packet is logged and dropped
- Firewall passes data *only* from classified scrubber interface over to government analysis station at far end
 - MAC filtering used to lower spoofing issues
 - Ruleset *only* passes data from Scrubber MAC to far-end analysis console
 - All other data logged and dropped by firewall



This Space Intentionally Left Blank

Testing & Documentation



- Concept of Operations Plan required for approval prior to everything
- Once ConOps approved, Government wanted a Test Plan submitted
- After Test Plan approved, Government attended test run of system without far-end connectivity
 - Send unacceptable packet from foreign system to packager
 - Document rejection
 - Send unacceptable packet to scrubber
 - Document log and reject
 - Send packet back from far-end back to UNCLASSIFIED side
 - Document packet scrubber log and reject
 - Document firewall refusal to communicate with other systems
- Results written up/submitted for final approval of live run

This Space Intentionally Left Blank

Credits



- Images

- Boognish: © Ween <<http://www.ween.com/>>
- The Man: © Kristen Ankiewicz <<http://www.monsters.net/>>

- OSS

- Snort_Inline – Rob McMillen (Jed Haille introduced me to it.)
 - <<http://snort-inline.sourceforge.net/>>
- Iptables/Netfilter – Harald Welte, Rusty Russell & The Netfilter Team
 - <<http://www.netfilter.org/>>



This Space Intentionally Left Blank