Live fire exercise:
Baltic Cyber Shield 2010

Kenneth Geers

Naval Criminal Investigative Service (NCIS)
Cooperative Cyber Defence Centre of Excellence (CCD COE)
Tallinn, Estonia

DEF CON 18

Overview

- May 10-11, 2010
- International cyber defense exercise (CDX)
- CCD CoE / Swedish National Defence College
- Six Blue Teams
  - Northern European gov, mil, priv, acad
  - Simulated power generation companies
- Red Team
  - Twenty hackers
- Scenario
  - Critical Information Infrastructure (CII)
  - Cyber terrorism

Introduction

- Are cyber attacks a threat to national security?
  - Cyber terrorism, cyber warfare
- Expert opinions
  - Dismissive to apocalyptic
- What would the targets be?
  - Electricity, water, air traffic control, stock exchange, national elections…

Trends

- National critical infrastructures increasingly connected to the Net
- Custom IT systems replaced with less expensive, off-the-shelf Windows and UNIX
- Networks Internet-enabled
- OS familiarity may facilitate hacking

Nat’l Security Thinking

- Cyber attacks: better understanding required
  - Some real-world case studies
  - Much information lies outside public domain
  - No wars yet between two Internet-enabled militaries
- Must be able to simulate cyber attack and defense in a laboratory

Moving Target

- IT, hacking are complex and dynamic
  - Rapid proliferation of computing devices, processing power, user-friendly hacker tools, practical encryption, Web-enabled intelligence collection
- Realistic CDXs are a challenge
  - Must simulate adversary, friendly forces, even the battlefield
  - Conclusions may be valid for a short time

Half-Life

- The military and computers
  - Train tank drivers, pilots
  - Simulate battles, campaigns, complex geopolitical scenarios
- Can a computer program model the real world?
- Failure factors
  - Poor intelligence, miscalculations, incorrect assumptions, scoring system, political considerations
  - 2002: $250 million Millennium Challenge

CDX Design

- Robust CDX requires team-oriented approach
  - Blue Team: friendly forces
  - Red Team: hostile forces
  - Green Team: technical infrastructure
  - White Team: game management

Blue Team

- Real-life system administrators and computer security specialists
  - Primary targets for instruction
- Goal
  - Defend network confidentiality, integrity, and availability (CIA) vs hostile RT
  - Scoring: automated and manual system

Red Team

- The cyber attacker
  - BCS: “cyber terrorist”
- Goal
  - *Undermine* CIA of BT networks
- Tactics
  - On virtual battlefield, almost no limitations
- “White box” vs “black box” testing
  - The question of prior knowledge

White Team

- Manages and referees CDX
  - Writes game scenario, rules, scoring system
  - Makes in-game adjustments
  - Tries to prevent cheating
    - EX: is a firewall rule detrimental to game or unrealistic in real-life?
  - Declares the “winner”

Green Team

- Designs, hosts network infrastructure
  - In-game ISP
  - Records traffic for post-game analysis
  - Manages automatic scoring
- Virtual machine technology
  - Technically possible with few resources
  - Simulating powerful adversary = many resources
    - EX: RT plan should indicate money, manpower
- VPN technology
  - The teams can be physically located anywhere

Cyber War Philosophy

- Cyber warfare is not traditional warfare
  - Tactical victories: reshuffling of bits
  - Then, any real-world effects?
- Cyber attack
  - Not an end in itself
  - Extraordinary means to many ends
    - Espionage, DoS, identity theft, propaganda, destruction of critical infrastructure

CDX goals

- The minimum
  - Credible simulation of network attack and defense
- RT vs BT
  - Same goals as any hacker and defender
  - Acquisition / prevention of *unauthorized access*
- Real-world impact
  - Political / military results?
  - Zip, minor annoyance or national security crisis?

Scenario

- Helps determine strategic significance
- Should estimate resources and cost
  - Lone hacker, group, or nation?
  - Can a lone hacker be a nat'l sec threat?
- Out-of-the-box thinking
  - Helpful…
  - …but may take real-world cyber attacks to change threat perception

Nation-state simulation

- Mil / gov agencies are “full-scope” actors
  - May not rely solely on computer hacking to achieve an important objective
  - Deep nat’l well of IT expertise
    - Cryptography, programming, debugging, vulnerability discovery, agent-based systems, etc
  - Supported in turn by experts in other disciplines
    - Natural sciences, physical security, supply chain, continuity of business, social engineering, etc

EX: Sandia Nat’l Labs

- Robust RT
    - Kills include military installations, oil companies, banks, electric utilities, e-commerce firms
    - Specialize in finding hidden vulns in complex environments
        - Obscure infrastructure interdependencies in highly specialized domains
- Former chief
    - “Our general method is to ask system owners: ‘What's your worst nightmare?’ and then we set about to make that happen”

CDX history

- Every CDX is unique
  - Good thing
  - Too many variables in cyberspace
  - IT evolves too quickly
- Some laboratory-based, others real-world
- Cyber defenders may be warned, may not

Eligible Receiver (1997)

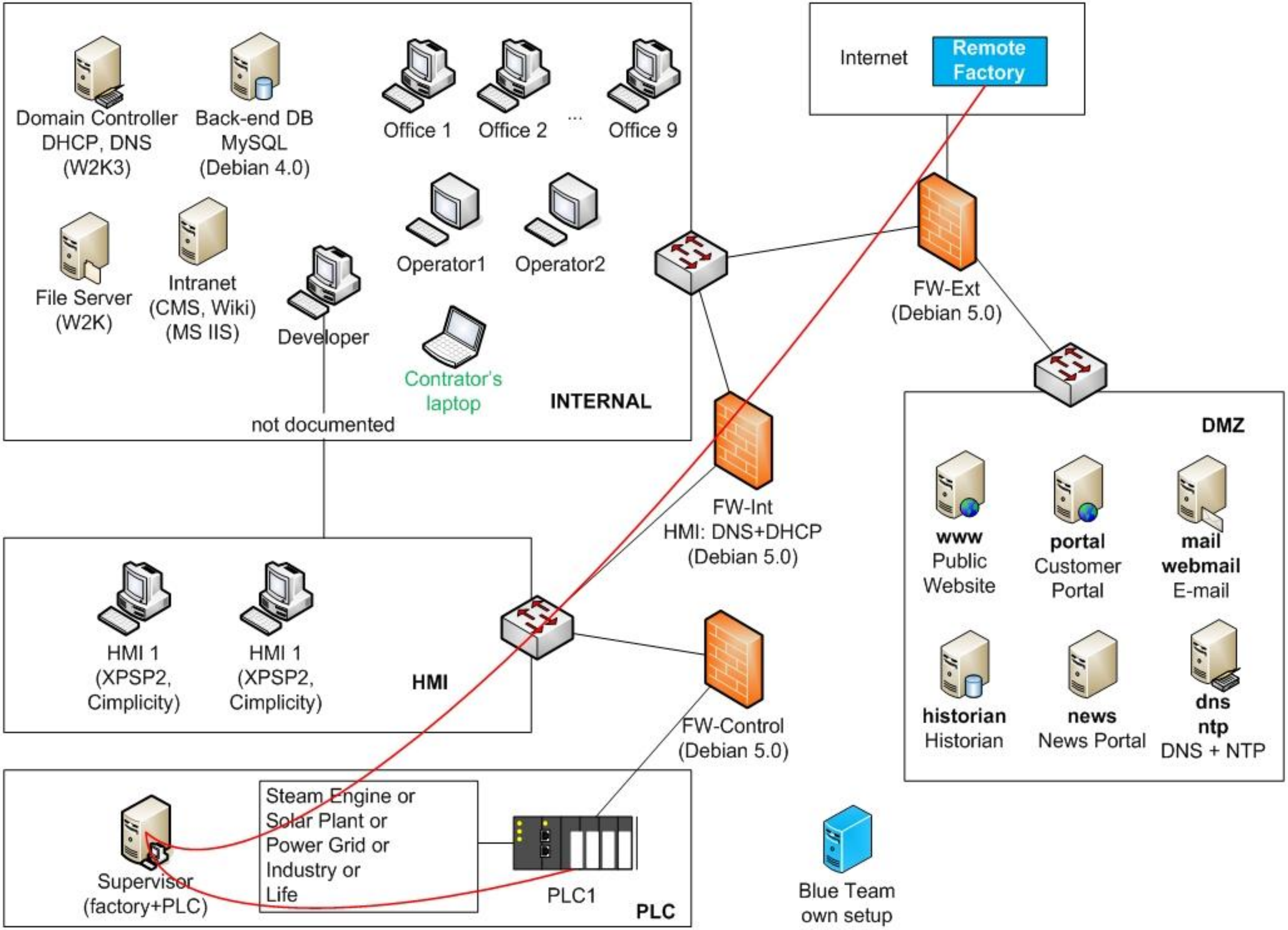
- RT: 35 NSA personnel
  - Assumed role of North Korean hackers
  - Targeted U.S. Pacific Command
- J. Adams in *Foreign Affairs*
  - “human command-and-control system” infected with “paralyzing level of mistrust”
  - “nobody in the chain of command, from the president on down, could believe anything”
- Also revealed that many national critical infrastructures are vulnerable to cyber attack

Water Security

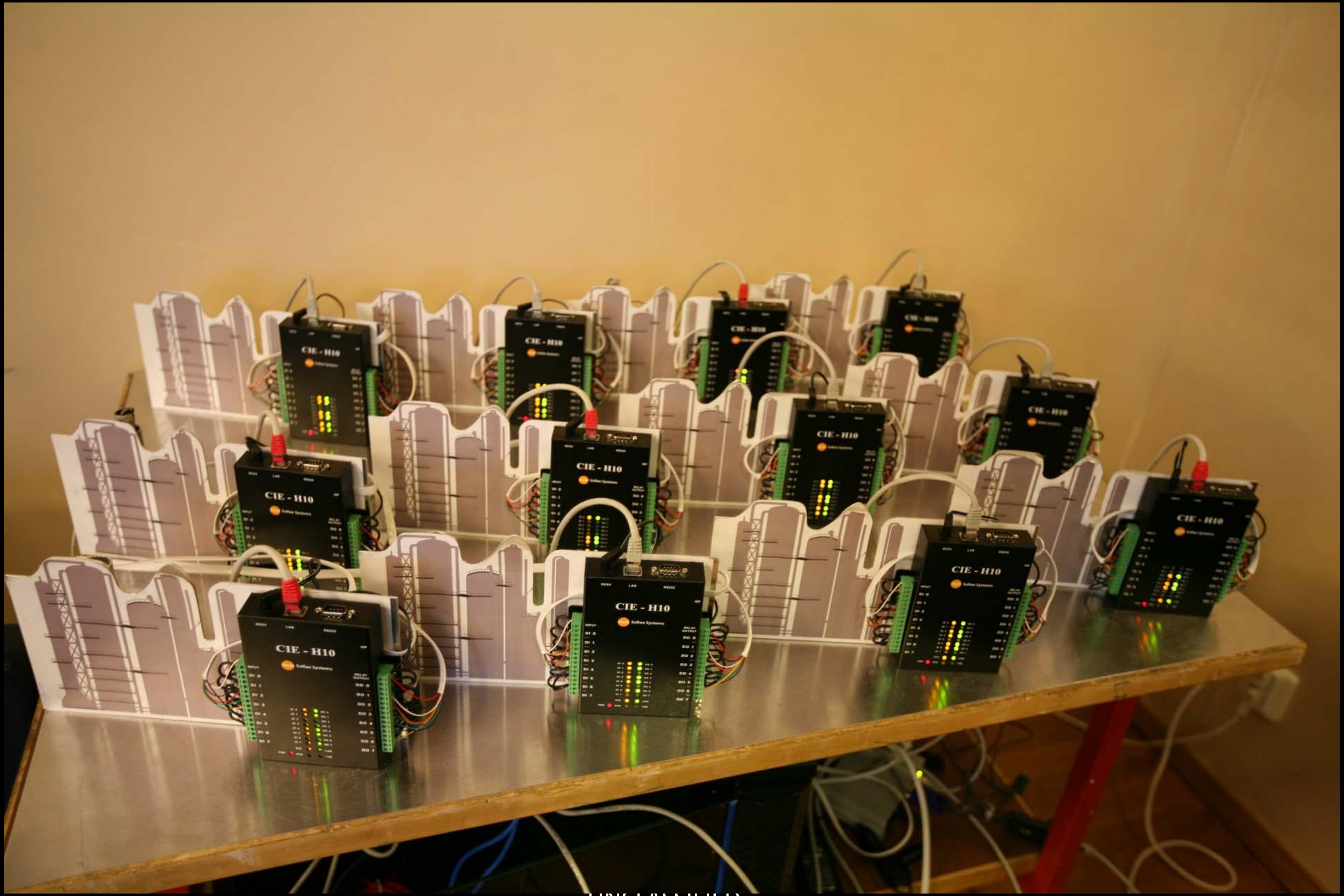
- 2006: Environmental Protection Agency
  - Could a hacker poison the water supply?
  - Sandia conducted vuln assessment of water dist. plants serving >100,000
    - 350 such facilities
    - Thorough analysis of 5 sites
    - Risk Assessment Methodology for Water (RAM-W)

International CDXs

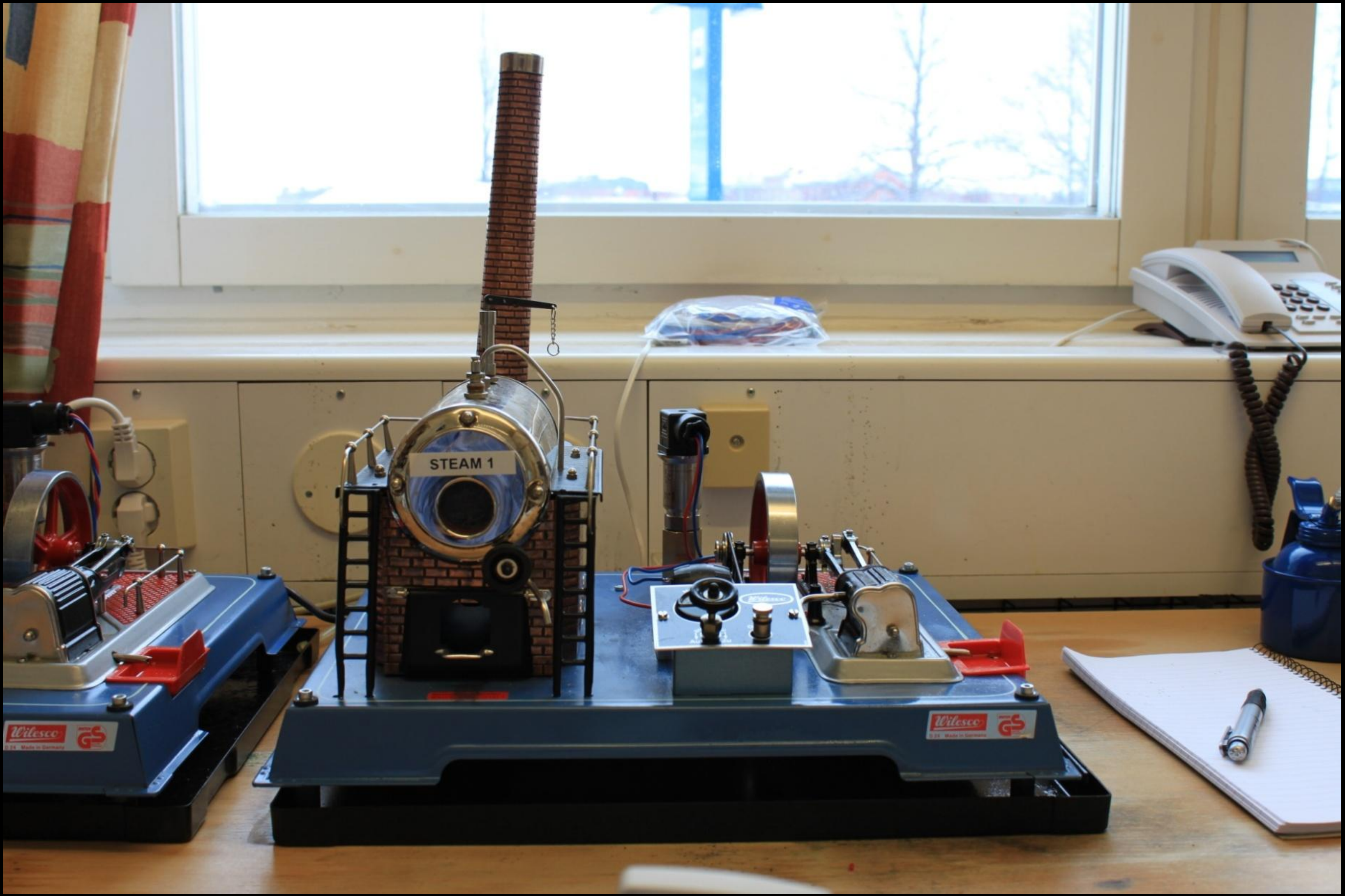
- Important trend
  - Internat’l architecture, internat’l responsibility
- 2006 DHS Cyber Storm
  - Scenario: non-state “hacktivists”
  - Gov agencies and the private sector
- 2008 Cyber Storm II
  - Scenario: Nation-state actor
  - Cyber & physical attacks on coms, chem, RR, pipe infrastr.
- 2009: CDX in remote and mountainous Tajikistan
  - U.S., Kazakhstan, Kyrgyzstan, Afghanistan

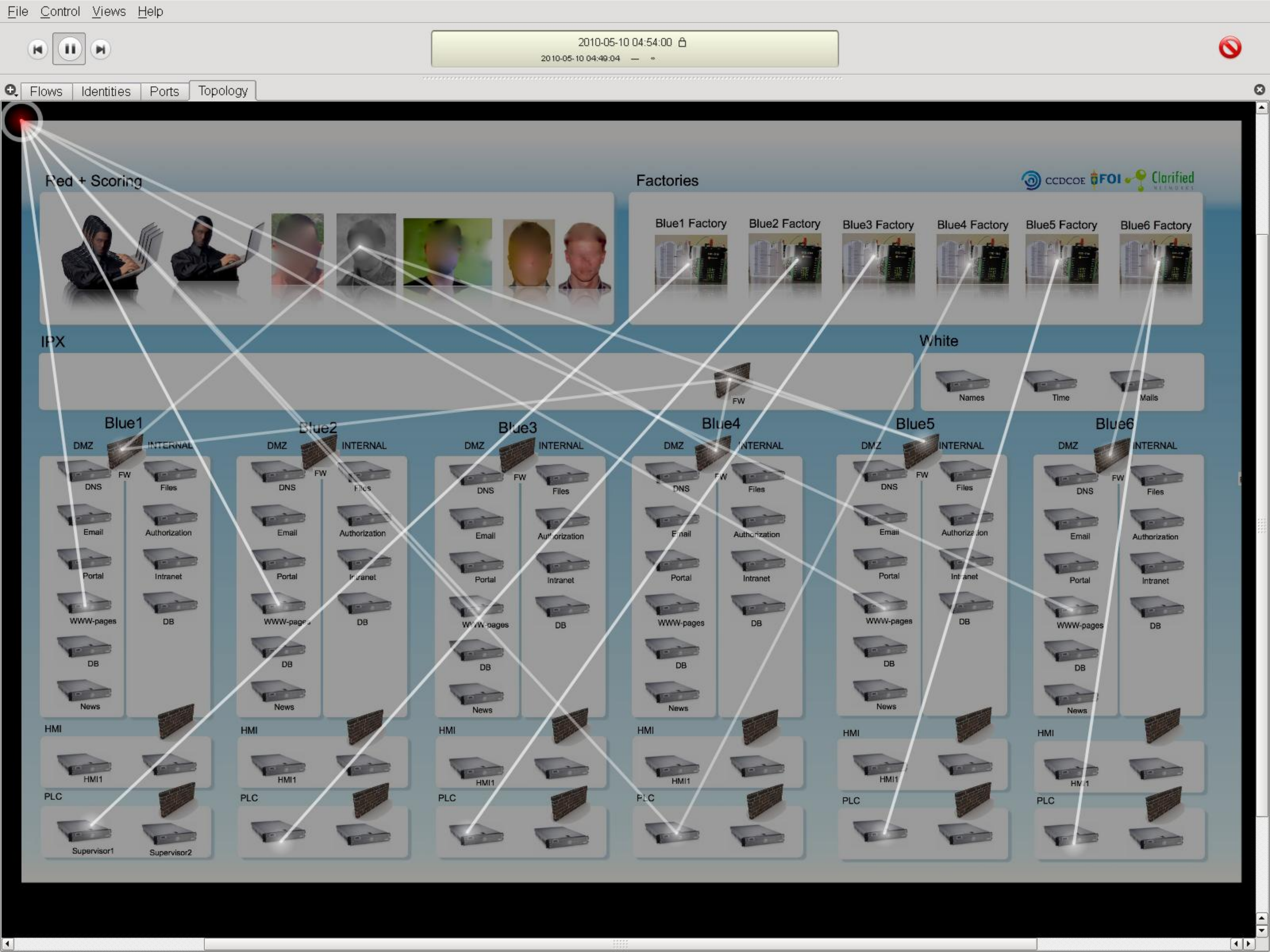

Domain Controller
DHCP, DNS
(W2K3)
Back-end DB
MySQL
(Debian 4.0)
Office 1
Office 2
...
Office 9
Internet
Remote Factory
File Server
(W2K)
Intranet
(CMS, Wiki)
(MS IIS)
Developer
Operator1
Operator2
FW-Ext
(Debian 5.0)
Contrator's laptop
INTERNAL
not documented
FW-Int
HMI: DNS+DHCP
(Debian 5.0)
DMZ
www
Public Website
portal
Customer Portal
mail
webmail
E-mail
HMI 1
(XPSP2,
Cimplicity)
HMI 1
(XPSP2,
Cimplicity)
HMI
FW-Control
(Debian 5.0)
historian
Historian
news
News Portal
dns
ntp
DNS + NTP
Steam Engine or
Solar Plant or
Power Grid or
Industry or
Life
Supervisor
(factory+PLC)
PLC1
PLC
Blue Team
own setup

Model Factories



Model Steam Engine




File
Control
Views
Help
2010-05-10 04:54:00
2010-05-10 04:49:04
Flows
Identities
Ports
Topology
Red + Scoring
Factories
CCDCOE
FOI
Clarified
Blue1 Factory
Blue2 Factory
Blue3 Factory
Blue4 Factory
Blue5 Factory
Blue6 Factory
IPX
FW
White
Names
Time
Mails
Blue1
Blue2
Blue3
Blue4
Blue5
Blue6
DMZ
INTERNAL
FW
DNS
Files
Email
Authorization
Portal
Intranet
WWW-pages
DB
News
HMI
HMI1
PLC
Supervisor1
Supervisor2

UNCLASSIFIED

Burning Down the House

- Still editing …
  - – will be fresh for D C 18 !!!

Baltic Cyber Shield

- 10-11 May 2010
  - – Numerous countries in northern Europe
  - – “Live-fire” CDX
  - – Twenty-person international RT
  - – Six national BTs
- Unscripted battle
  - – Use of malicious code authorized and encouraged
    - Within the confines of a virtual battlefield

- BCS 2010 similar to annual U.S. military CDXs
- Pentagon’s International Cyber Defense Workshop (ICDW)
- UCSB International Capture the Flag (iCTF)
- U.S. National Collegiate Cyber Defense Competition

- Scenario
  - Volatile geopolitical environment
  - Newly hired network security team
  - Defended power supply company’s CII networks
  - Adversary: non-state, terrorist group
  - Attacks grew in sophistication throughout CDX

- Three primary goals
  1. BTs should get hands-on training in CII defense with elements of Supervisory Command and Data Acquisition (SCADA) infrastructure
  2. CDX should highlight international nature of cyberspace: political, institutional, legal, etc
  3. Everyone should gain a better understanding of how to conduct CDXs in the future

- WT: CCD CoE in Tallinn and SNDC in Stockholm
- Scoring criteria
  - Gauged BTs’ ability to maintain CIA
    - Office infrastructure and external services
  - Negative points depended on criticality of system, service, compromise
    - ie, Admin/Root-level access, compromised SCADA Programmable Logic Controller (PLC) carried big penalties
  - Positive points
    - Thwarted attacks, completing “business requests,” implementing innovative strategies and tactics

- Six BTs
  - 6-10 personnel each
  - Northern Euro gov, mil, priv sec, academia
- All given identical, pre-built, somewhat insecure network
  - 20 physical PC servers, 28 virtual machines
  - 4 VLAN segments: DMZ, INTERNAL, HMI, PLC
  - Also connected to in-game “business” servers

- Scenario included SCADA software
  - Should simulate power generation company’s production, management and distribution capabilities
  - GE PLCs, Simplicity HMI terminals, Historian databases
  - Two physically-separated model factories per BT network

- BTs given access to CDX environment one month prior
  - And “outdated” network documentation
- BTs could harden their networks
  - But a minimum number and type of applications and services had to be maintained
- Could install new software and/or modify existing software
  - But offensive BT cyber attacks (on RT or other BTs) strictly prohibited

- RT: twenty volunteers
  - WT directed RT to begin slowly and gradually increase attack scale and sophistication
  - No other limits on hacker tools and techniques against BTs
- RT strictly prohibited from attacking CDX infrastructure
- All attacks confined to CDX environment
- Internally, RT divided into four sub-teams
  - “Client-side”, “fuzzing”, “web app”, “remote”

- GT: Swedish Defence Research Agency (FOI)
  - Linköping, Sweden
  - Hosted most of BCS 2010 infrastructure
  - BT nets designed by GT / WT
  - FOI laboratory: 9 racks, 20 physical servers each
- Game infrastructure included 12, 20-centimeter-tall physical models of factories
  - Each had PLC, SCADA SW, 50-centimeter butane flame
    - RT could turn on as “proof” of a successful attack
- RT / BTs accessed game via OpenVPN

- WT had robust visualization environment
  - Network topography
  - Traffic flows
  - Observer reports
  - Chat channels
  - Team workspaces
  - Scoreboard
  - Terrestrial map of the game environment

BCS execution

- Formal start
  - BTs / RT login
- Fun begins
  - RT begins the cyber attack

- The RT campaign had four phases
  1. Declaration of war
  2. Breaching the castle wall
  3. Owning the infrastructure
  4. Wanton destruction

- Declaration of war
  - RT defacement of each BT public websites
  - Delivery to power company of ultimatum
    - Extremist environmental organization “K3 Cyber warfare division”
    - Company must immediately cease its operations and convert to alternative, greener power or face crippling cyber attack
    - RT defaced 5 of 6 sites in 30 minutes

- Phase one
  - RT only allowed to compromise one server in each BT DMZ and one internal workstation
- RT still created a steady stream of incident reports
  - WT had trouble scoring them all
  - EX: within 1 hour, RT had live A/V feed into one BT workspace

- Historical CDX challenge
  - Difficult for RT to maintain balanced and sustained pressure on all BTs
  - WT directed RT that for each vulnerability discovered, all BT systems must be systematically checked

- Phase two
  - RT should compromise as many DMZ systems as possible
  - End of day one: RT successfully attacked 42 computers, including web and email servers

- Phase three
  - BT “crown jewels”
    - Internal network computers providing Human Machine Interface (HMI) for power generation and management, i.e. SCADA infrastructure
  - RT claimed only limited victories
    - Only 1 of 12 model factories set on fire
      - And was it intentional or accidental?

- Phase four
  - “Wanton destruction”
  - RT could attack and destroy any BT system
  - Goal: desperate K3 attempt to cause maximum disruption to the power companies’ operations
- Not a wise CDX decision!
  - RT often denied service to previously conquered systems
    - EX: Custom-configured Cisco router used to simulate traffic denied RT access to the CDX for 15 minutes
  - Prevented WT from accurately scoring the game

- Publicly-known vulnerabilities
  - MS03-026, MS08-067, MS10-025, flaws in VNC, Icecast, ClamAV, and SQUID3
- Hacked web applications
  - Joomla and Wordpress
  - SQL injection, local / remote file inclusion, path traversal, cross-site scripting vs Linux, Apache, Mysql, PHP
- Other tactics
  - Account cracking, online brute-forcing, DoS with fuzzing tools, password hash-dumps , “pass-the-hash”
  - Backdoors: Poison Ivy, netcat, custom-made code
  - Metasploit used to deploy reverse backdoors
  - Altering crontab to drop firewall rules
  - ** One zero-day client-side exploit for most browsers **

- Only the BTs were scored…
  - But RT compromised over 80 BT computers

- BT successful defensive strategies
  - BCS 2010 winner
    - Did not prioritize patching vulnerable systems or fixing hacked computers
    - Moved essential services like NTP, DNS, SMTP, WebMail to their own, custom-built, higher-security virtual machine
    - Requested “out-of-band” communications w/ WT
      - Did not trust in-game e-mail

- Successful OS-hardening tools and techniques
  - Linux: Samhain, AppArmor, KernelGuard, custom short shell scripts
  - Windows: SE46 Computer Integrity System, central collection of event logs
  - All OSs: blocking and black hole routing of offending IP addresses

Conclusion

- CCD CoE / FOI assess three primary goals accomplished

First

- BCS infrastructure allowed for a “live fire” CDX
  - Gave 6 BTs opportunity to defend CII / SCADA
  - All teams reported no down-time
  - Scenario offered a glimpse of a “cyber terrorist” threat that may be more realistic than we suppose

Second

- BCS 2010 was a truly international exercise
  - Cyber attacks can be launched from anywhere in the world, so it is critical to develop cross-border relationships now
  - Over 100 personnel from 10 countries participated

Third

- Post-game survey
  1. Strength-test all connectivity well before a CDX
  2. Make rules and scoring crystal clear to everyone
  3. Allocate significant manpower to the WT for communication, scoring and adjudication
  4. In a project this big, be ready for clashing egos and agendas
  5. Avoid the “wanton destruction” phase
  6. Do not underestimate the amount of time required to prepare for a robust CDX

- Many CDX challenges mirror the real world
  - Cyber defenders may never see the same attack twice
    - IT and cyber attacks are too complicated, have too many variables, evolve too quickly
  - The intangible nature of cyberspace can make the calculation of victory, defeat, and battle damage a highly subjective undertaking
    - Even knowing whether one is under attack can be a challenge!

References

Adams, J. (2001). “Virtual Defense,” Foreign Affairs 80(3) 98-112.
“Air Force Association; Utah's Team Doolittle Wins CyberPatriot II in Orlando.” (2010, Mar 10). De-fense & Aerospace Business, p. 42.
Bliss, J. (2010, Feb 23) “U.S. Unprepared for ‘Cyber War’, Former Top Spy Official Says,” Bloomberg Businessweek, online.
Caterinicchia, D. (2003, May 12) “Air Force wins cyber exercise.” Federal Computer Week, 17(14), p. 37.
Chan, W. H. (2006, Sep 25). “Cyber exercise shows lack of interagency coordination.” Federal Com-puter Week, 20(33) p. 61.
“Cyber War: Sabotaging the System.” (2009, Nov 8). 60 Minutes: CBS.
Geers K. (2010). “The challenge of cyber attack deterrence.” Computer Law and Security Review 26(2) pp. 298-303.
Geers, K. (2008, Aug 27). “Cyberspace and the Changing Nature of Warfare.” SC Magazine.
Gibbs, W. W. (2000). “RT versus the Agents.” Scientific American, 283(6).
Goble P. (1999, Oct 9). “Russia: analysis from Washington: a real battle on the virtual front.” Radio Free Europe/Radio Liberty.
Gomes, L. (2003, Mar 31). “How high-tech games can fail to simulate what happens in war.” Wall Street Journal.
Gorman, S. (2009, Aug 17) “Cyber Attacks on Georgia Used Facebook, Twitter, Stolen IDs.” Wall Street Journal.
“International cyber exercise takes place in Tajikistan.” (2009, Aug 6). BBC Monitoring Central Asia. (Avesta website, Dushanbe)
Keizer, G. (2009, Jan 28). “Russian ‘cyber militia’ knocks Kyrgyzstan offline.” Computerworld.
Lam, F., Beekey, M., & Cayo, K. (2003). “Can you hack it?” Security Management, 47(2), p. 83.
Lawlor, M. (2004). “Information Systems See Red.” Signal 58(6), p. 47.
Lewis, J.A. (2010) “The Cyber War Has Not Begun.” Center for Strategic and International Studies.
Meserve, J. (2007, Sep 26). “Sources: Staged cyber attack reveals vulnerability in power grid.” CNN.
Orr, R. (2007, Aug 2). “Computer voting machines on trial.” Knight Ridder Tribune Business News.
Preimesberger, C. “Plugging Holes.” (2006). eWeek, 23(35), p. 22.
“Remarks by the President on Securing our Nation's Cyber Infrastructure.” (2009). The White House: Office of the Press Secretary.
“Tracking GhostNet: Investigating a Cyber Espionage Network.” (2009). Information Warfare Moni-tor.
Verton, D. (2003) “Black ice.” Computerworld, 37(32), p. 35.
Verton, D. (2002). The Hacker Diaries: Confessions of Teenage Hackers. New York: McGraw-Hill/Osborne.
Wagner, D. (2010, May 9). “White House sees no cyber attack on Wall Street.” Associated Press.
Waterman, S. (2008, Mar 10). “DHS stages cyberwar exercise.” UPI.
“‘USA Today’ Website Hacked; Pranksters Mock Bush, Christianity.” (2002, JUL 11). Drudge Report.