Securing the End Node in a Cloud World

Lt Col Ken Edge, PhD
Electronic & Net-Centric Warfare Division
Air Force Research Laboratory

Approved for Public Release: RY-11-0022, 88 ABW-11-0375
Of Clouds and Nodes

How?

You trust your Network?    Network trusts you?
You trust your PC?          Network trusts your PC?
Air Force Research Laboratory,  
Wright Patterson AFB,  
Sensors Directorate,  
Integrated Electronic and Net-centric Warfare Division  
  – Full spectrum electronic warfare attack and protection technology  
    *R&D of radio frequency hardware and software*  
  – RF testing and assessments  
    *Jamming, shielding, RF interference with medical gear, etc.*  
  – Synthetic and virtual simulation labs plus an avionics testbed  
    *Very high fidelity testing of future and real-world components*  
  – Architectures of Trusted Complex Systems  
  – 6 Branches, ~170 persons, ~100 advanced degrees

*Full spectrum, world dominant electronic and cyber warfare R&D*
AT-SPI Technology Office

• **RYWA Branch**
  – 10+ years
  – ~35 civilians/military/contractors
  – Theory, research, design, prototypes, outreach, assessments

• **DoD Software Protection Initiative, spi.dod.mil**
  – Anti-piracy, anti-modification, anti-reverse engineering
  – R&D focused, rapid build and deploy prototypes
  – OPR for all DoD

• **DoD Anti-Tamper Field Office, at.dod.mil**
  – Prevent exploitation, slow technology proliferation
  – Legacy and new weapon systems
  – SAF/AQL Executive Agent

Blended SW and HW solutions
Our Approach

• The Threat
  – Nation-State with unlimited resources
  – Both over-the-wire and physical access
  – Root privilege and insider design knowledge

• The Environment
  – Realistic, COTS technology
  – Global Access
  – Limited resources, cost

• Design and Engineering

• The Assessment
  – Unconstrained, professional hackers attack
  – Physical and logical, penetration and exploitation teams

Our Goal: Integrate ‘trust’ into COTS IT
Vulnerability is the *intersection* of three elements:

1. System Susceptibility
2. Threat Accessibility
3. Threat Capability
AT-SPI’s Three Security Tenets

1. Focus on What’s Critical  (shrink susceptibility)
   – Define mission needs, access points
   – Remove unnecessary parts
   – Minimize potential access points

2. Move It Out-of-Band  (restrict threat access)
   – Constrain necessary access to sensitive data

3. Detect, React, Adapt  (deny threat capability)
   – Countermeasures
   – Inside Threat’s OODA loop
   – Impose penalties when attacked
   – Fight through the attack!

Vulnerability
Range of R&D

Fundamentals
Soft/Firmware defenses
Vulnerability Analysis
Unique Labs

Enterprise Solutions
Sensor command/control
Malware research
Internet browsing

Protecting Software
Creation
Sharing
Execution

Mobile Solutions
Up next
Spectrum of Secure End Nodes

Availability

Confidentiality

Greater Security

Encryption Wizard

Lightweight Portable Security

Secure Mobile Environment

SMD netbook

Secure Knowledge Gateway

Protect Files

Remote Access Apps

OS

Store Data Apps

RTE

AT Hardware

Access Data Apps

RTE

Download Data, OS

Local use AT Hardware
Encryption Wizard

- Free
- Java applet
- 1.4 Mb (Portable)
- 128-bit AES
- Files and Folders
- CAC / PassPhrase

- Granular file, data-at-rest, data-in-transit protection
- Licensed FIPS 140-2
- Certified by Army & AF for NIPRNet and SIPRNet
- +66k Government users
Lightweight Portable Security

- Instant trusted end-node
- CAC-enabled
- Safe browsing
- Safe enterprise access

- Use almost any computer
- Lightweight Linux OS boots from CD
- Runs only in RAM
  - Cannot mount local harddrive
  - Leaves no local traces

Recipient of DoD CIO award
**LPS-Public**

Lightweight Portable Security – Public Edition

---

**Features**

- Free! Download, burn, and run today
- Safely browse risky and sensitive sites
- CAC enabled (reader required)
- Leave no local traces (or malware)
- Deluxe: OpenOffice productivity suite

**Tenet #1: “Focus on the Critical”**

- Bypasses untrusted OS + hard drive
- Focused on running browser

**Tenet #2: “Move It Out of Band”**

- Temporal, pristine OS from boot CD

---

As seen on AF Portal and Slashdot.
LPS-Remote Access

Features
• Very low-cost, fast telework solution
• Safe remote access to enterprise network
• Customized for existing networks
• An ‘in-pocket NIPRNet desktop’
• Accredited; AF E/APL, Army CoN

Tenet #1: “Focus on the Critical”
• Create trusted “virtual GFE” end node

Tenet #2: “Move It Out of Band”
• CD creates temporal ‘out of band’
• All sensitive data remains on servers

Approved DoD-wide by DoD CIO for COOP, AF-wide for daily use
DISA / USCYBERCOM DoD-wide telework pilot in progress
Secure Mobile Desktop

Tenet #1: “Focus on the Critical”
• Trusted, simple end-node
• Near-zero maintenance, updates

Tenet #2: “Move It Out of Band”
• Sensitive data remains on server

Tenet #3: “Detect, React, Adapt”
• Tampering denies access

Features
• Fast and focused COTS netbook
• Immutable Run Time Environment
• Secure remote network access
• Stolen? No data compromised
• CAC enabled; encrypted comms
• Inexpensive or ruggedized

Operational pilots in progress
Secure End Node (NSA Type I)

- **Technical Approach**
  - Customized Secure End Node issued to operators
  - Hard drive removed and replaced with immutable read only device that is ‘unhackable’.
  - Integration of external hardware encryptor (NSA approved up to TS/SCI) allows laptop to be handled as CCI rather than classified when not keyed.
  - Power, compute device, encryptor, anti-tamper, and case integrated into single portable package for ease of use and transport
  - Type 1 accreditation readily achieved
Secure Tablet

Dual-Use Device for Partitioned Access to Public Networks and Mission Networks
Summary

• We research and develop tailored solutions to protect critical intellectual property

• Unique, trusted, easily deployed, and cost effective solutions based on COTS

• Secure End Nodes are available today

• *Challenges Welcome!*
  – Bring us your Tough Problems
  – Seeking organizations to partner with to develop/deploy leading edge protection technologies
QUESTIONS?

Electronic & Net-Centric Warfare Division, Air Force Research Laboratory

spi.dod.mil
Kenneth.edge@wpafb.af.mil