SAND2015-4241C

Pacific Northwest NATIONAL LABORATORY

Proudly Operated by Battelle Since 1965

Computer Security in an Increasingly Mobile World

Z.N. GASTELUM[1], J.R. DOEHLE[2], E.T. GITAU[3]

[1]Sandia National Laboratories
Albuquerque, NM, USA

[2]Pacific Northwest National Laboratory
Richland, WA, USA

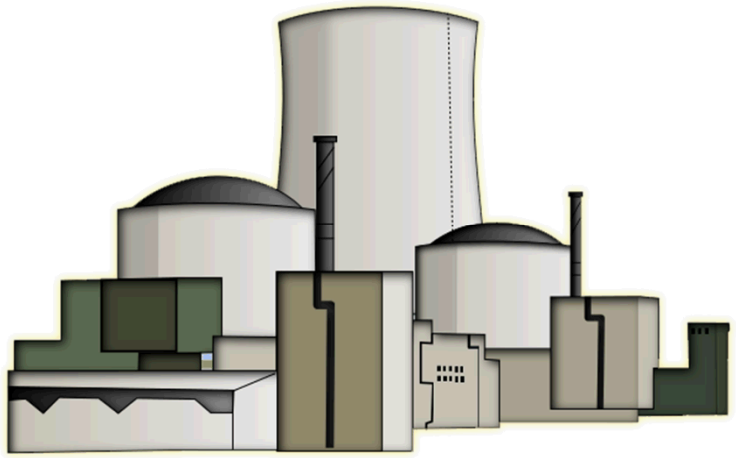
[3]Pacific Northwest National Laboratory
Seattle, WA, USA

U.S. DEPARTMENT OF ENERGY

Computer and Information Security Concerns of Mobile Devices in the Nuclear Field

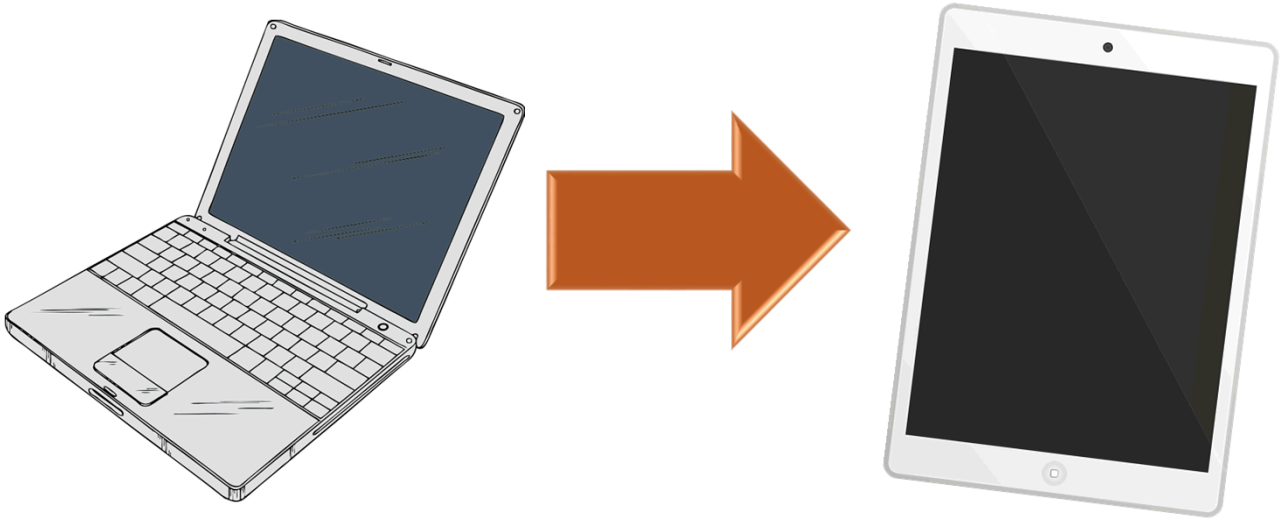
Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Two International Safeguards Scenarios
  - Base Case
  - Expanded Case
- Identify information and computer security concerns
- Propose general mitigation strategies
- Offer applications relevant to other mobile technology users in the nuclear field



Base Case: Tablet Computer Replacing Inspector Laptop

- Mobile device will be a tablet computer
- Tablet will replace inspector laptop
  - Required to run all software currently used on laptop
- Data connections will be conducted wirelessly
- Tablet will not replace safeguards verification equipment



Computer and Information Security Concerns (Base Case)

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Network Connections and Data Transmission
  - Wireless connection inherently less secure than wired
  - Confidentiality and integrity concerns
  - Vulnerability from network being used to access Internet
- Data Storage and Processing
  - Data brought from IAEA Headqua
    tablet could be viewed and altere
- User-Generated Security Concern
  - Users play critical role: can expos
  - Tablets will likely be used for pers
    laptops currently are
    - Can expose devices to threats re

Computer and Information Security Concerns (Base Case)

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Transnational Information Security
  - Multi-country inspection trips require transporting multiple countries' safeguards-relevant data
    - Can make an enticing target
  - Information security concerns for i networks
    - A compromised device can transf
- Safeguards-Specific Issues
  - Authentication keys on device for
  - Mobile technologies would likely r Safeguards Environment

Mitigation Strategies (Base Case)

- Encryption
  - Currently: laptops have full-disk encryption
  - Disk encryption is common feature on most major tablet platforms
  - Virtual Private Network (VPN) to address insecure wireless network connection
- Remote Wiping
  - Application-, manufacturer-, or se
  - Mandatory “check-in” policy to en

Mitigation Strategies (Base Case)

- User Permissions
  - Current use of laptops is business and personal on same device
    - Would likely continue for tablets
  - Laptop hard drives are partitioned to separate official data from personal use
    - Tablets would likely use a softwar
- Training and Security Practices
  - Critical for users to be trained on l controls put in place
    - Can be a challenge given the diffe
  - Practice effective security in main
    - Timely updates and patching, anti

Expanded Case: More Technologies and Further Integration

Pacific Northwest NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Additional technologies
  - Smart phone, smart watch, wearable cameras, other wearable technology
- More complex data management system
  - Provide access to documents and reporting; live tasking support from Headquarters
- Global Positioning System capabi
  - Navigation and situational awaren
    Verification or Complementary Ac
- Integration with IAEA safeguards
- Inspector travel support
  - Voice-to-text language translation support

Computer and Information Security Concerns (Expanded Case)

- Broader Attack Surface
  - Each additional technology is a distinct platform that must be secured
  - Increased connectivity between devices could put more devices and information at risk from a single device's vulnerability
  - Increased availability of informatic
- System Availability
  - Highly connected feedback loops in field and at IAEA Headquarters concern

Mitigation Strategies (Expanded Case)

- Additional Training
- IAEA Safeguards Equipment Authorization process
  - May be required if mobile device fundamentally integrates with safeguards equipment
  - Includes usability and safety testir other verification
- Additional and alternative authenti
  - E.g., biometrics

Recommendations for Nuclear Community

Deploy the minimal necessary mobile technologies to meet the prescribed use case

Train users

Prioritize connection to secure networks

Engage with industry

Thank you

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Joel Doehle

+1 509 375-2748
joel.doehle@pnnl.gov

Global Security Technology and Policy

www.pnnl.gov