Information ASSURANCE SPECIALISTS

Information Assurance, why we ALL need to know what it means…

Presented by
Keir Tomasso
IA Specialists, Inc.
PO Box 8944
Turnersville, NJ 08012
www.IASpecialists.com

Information Assurance… What Does Really Mean?

- Wikipedia – “**Information Assurance (IA)** is the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. Information assurance includes protection of the integrity, availability, authenticity, repudiation and confidentiality of user data. It uses physical, technical and administrative controls to accomplish these tasks.” [1]

- Information Assurance is a whole lot more then encrypting your emails and telephone conversations

[1] http://en.wikipedia.org/wiki/Information_assurance

Integrity, availability, authenticity, repudiation and confidentiality

- **Integrity** – Has the information been modified or tampered with in any way?

- **Availability** – Is access to the information always there where and when its needed?

- **Authentication** – Is the source of the iInformation who I think it is, or intend it to be?

- **Non repudiation** – Am I able to provide proof the information is genuine?

- **Confidentiality** – Are any unauthorized individuals also looking at my information?

Information Assurance Means different things to different types of information

- The US Gvt. and DOD implement Information Assurance controls over many forms of information
  - Sensitive but Unclassified and Classified voice
  - Sensitive but Unclassified and Classified emails/business networks
  - Sensitive but Unclassified and Classified video
  - Sensitive but Unclassified and Classified data
    - Intelligence information, etc.
  - Sensitive but Unclassified and Classified C2 – Command and Control
  - Etc…
- The DOD spends billions of dollars on robust Information Assurance technology, resources and man power
- This is all done to keep the “enemy” at bay…

So Who Really is the Enemy?

9/27/2013 - “U.S. Says Iran Hacked Navy Computers!!” [1]

9/26/2013 - *“Chinese Hackers Linked to Internet Explorer Breach”* [5]

9/19/2013 - “Hackers-for-hire: Chinese group accused of economic espionage against US companies” [4]

8/23/2013 - *“Iranian Hacker group claims credit for DDoS Attack on Nasdaq”* [3]

7/16/2013 - “Nuclear Proliferation Prevention Project (NPPP): U.S. Nuclear Facilities Vulnerable to Terrorist Attack” [2]

2010 – **And how can we forget about Stuxnet????**

[1] http://online.wsj.com/article/SB10001424052702304526204579101602356751772.html
[2] http://blogs.utexas.edu/nppp/files/2013/07/INMM-2013-July-paper.pdf
[3] http://hackersnewsbulletin.com/2013/08/iranian-hacker-group-claims-credit-ddos-attack-nasdaq.html
[4] http://rt.com/usa/hackers-china-hidden-lynx-092/
[5] http://blogs.wsj.com/digits/2013/09/26/chinese-hackers-linked-to-internet-explorer-breach/

The enemy can be anyone… a government, a hacker group, even an individual hacker!
Cyber warfare is REAL!

- Cyber warfare is so real that in 2006 the DOD announced the formation of a military organization to counter the ongoing cyber threat to the United States of America
  - Provisional status Nov. 2006, USCYBERCOM officially formed on June, 23rd, 2009
- In 2006 Congress also created The Department of Homeland Security Office of Cybersecurity and Communications
  - http://www.dhs.gov/office-cybersecurity-and-communications
- Both organizations provide US industry outreach, assistance, and guidance
  - DHS being the most open to industry in an effort help combat cyber espionage

Meanwhile… Back in Industry…

- Over time, the public sector & industry has realized the many benefits of permanently “connected” systems
  - Less manpower
  - More timely information/feedback
  - More granular information then every before
  - All contributing to positive effects/benefits of implementing technology
- Being such a large potential growth market, In July 2013 Cisco Systems formed a new business (500 person) unit called the “Internet of Things” business unit
  - Cisco feels that a new technology market is coming, worth upward of $14 trillion dollars
  - “Smart” appliances, supervisory control and data acquisition (SCADA) industrial controller systems, various sensors, broader and even deeper levels of automation systems, new consumer electronics goods, etc. will all create the need for new networking technologies, appliances, and capabilities

Cyber Threat and “Internet of Things” collide…

- New/more “always connected” technologies are on the horizon
  - So much so that industry giant Cisco is gearing up…
- Cyber warfare is REAL! The threat is global, the attack vectors are diverse, and it is happening around us 24x7
  - Economic Espionage, Industrial Espionage, etc.
- With new technologies, and new threats, comes new IA concerns…
- How will Industry react?
  - Proactive? or Reactive?

Industry... its time to embrace a holistic IA vision!

- The days of thinking “no one cares about that IP network based pump sensor” need to END!
- Protecting your information needs extend from “enterprise business networks” all the way down through ALL of your IP based/always on technology
- ALL IP based technology needs to be protected!!!!
  - Sensors
  - SCADA
  - IP Cameras
  - Access Control Systems
  - Etc.

IP Network Protection

- Using a VPN/tunneling technology to obfuscate your information doesn’t do a complete job to combat the cyber threat, and in some applications using a VPN/tunneling technology isn’t even a viable option

- Additional tools and security systems should be implemented, i.e.
  - Network isolation/limitation of access
    - Sure stovepipe networks are harder to manage, but they are more secure in the overall effort to protect your information
      - If your IP camera network has been exposed, does your SCADA run on the same network? It better not!
  - Intrusion Detection and Intrusion Prevention security technologies should be used
    - You may think it is pointless to use such tools on a stovepipe sensor or access control network, but wouldn’t you like to know if someone is playing “man in the middle” on your sensor data or access control system?
  - Don’t settle for “it can’t be done” when considering securing various technologies
    - Implementing security isn’t always easy, and it may cost a little more, but in the end its worth the additional cost burden as a breach or Information leak has economic impact for years and years after it takes place

my Suggestions…

- Don’t be afraid to leverage open source, or products based on open source
  - Just because its open source doesn’t mean its has vulnerabilities, actually quite the opposite is usually true
- Don’t be afraid to leverage products from companies other then Cisco
  - Cisco isn’t always the most secure, nor the most cutting edge
- Look for security solutions that talk about:
  - NIAP (National Information Assurance Partnership)
  - FIPS-140 (Federal Information Processing Standard -140 ~ security spec.)
  - FIPS-197 (Federal Information Processing Standard -197 ~ AES crypto spec.)
  - HAIPE Sec. / IMPEIR (NSA’s IP security specification for Suite B crypto implementation)
- Just because they say NSA Suite B crypto, or AES, doesn’t mean they are good… if they say they are IPMEIR Compliant, or use a FIPS-140 validated crypto module, they are talking the talk…

Take-Away Bullet Points

- Get smart on Information Assurance, and do so NOW!
- Stay vigilant, do not become complacent with your security appliances and tools, the threat is NEVER going away and the bad guys are always improving their skills/attack methods
- Ignorance is not bliss, if you don’t embrace implementing a holistic IA approach you WILL suffer the consequences sooner or later
- Lastly, demand more from your technology, your vendors, and your networks…

Time for a Shameless Marketing Plug…

- IAS provides IA related consulting services (electronics design, network, application, and test engineering services) to industry, government, and military customers

- IAS also offers a family of robust, uber small form factor, diverse WAN technology routers that feature NSA Suite B IPSec (HAIPE IPMEIR) VPN capabilities, Deep Packet Inspection, and Intrusion Detection and Intrusion Prevention Security capabilities
  - IAS Routers are both hardware appliances and embeddable software
    - Virtual machine versions AND port-able embeddable Linux code

Resources for additional information on the Cyber threat

- United States Computer Emergency Readiness Team (US-CERT)
  - http://www.us-cert.gov/nccic
- MANIANT
  - https://www.mandiant.com/resources/m-trends/
- US DOD CYBERCOM
  - http://www.defense.gov/home/features/2013/0713_cyberdomain/

Thank you for your time!

Information
ASSURANCE
SPECIALISTS

Presented by
Keir Tomasso
IA Specialists, Inc.
PO Box 8944
Turnersville, NJ 08012
www.IASpecialists.com