Distributed Security Operations Use Case

Roman Danyliw <rdd@cert.org>

MAMI Management and Measurement Summit (M3S)

March 16, 2018

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM18-0355

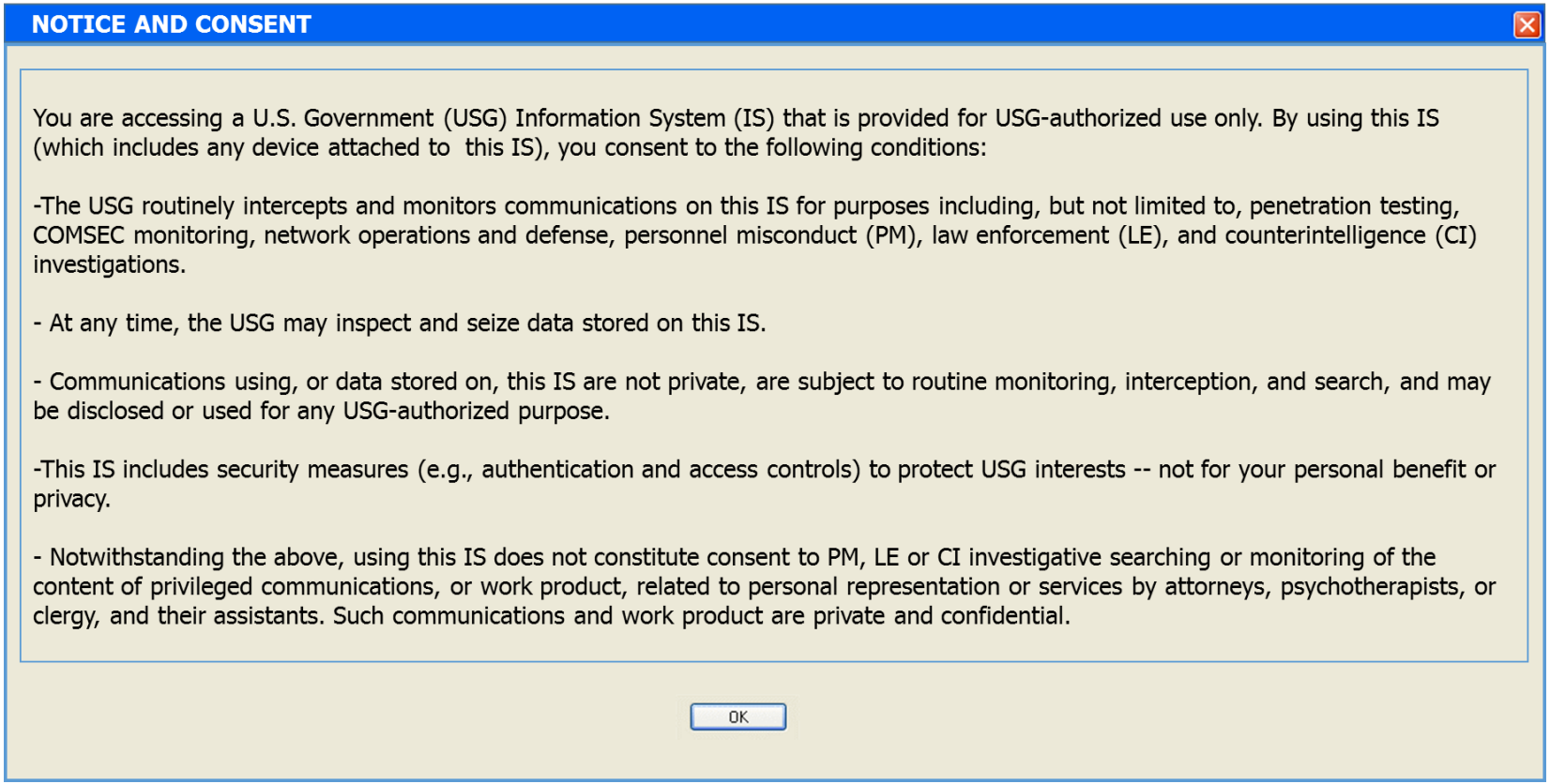
Software Engineering Institute

A DoD R&D FFRDC operated by Carnegie Mellon University

Mission

To support the Nation's defense by advancing the science, technologies, and practices needed to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring

CERT



Source: [DOD-CIO-CONSENT]

Operating Model of Use Case

Provide value-add to existing security operations [EINSTEIN2-PIA] [EINSTEIN3A-PIA]

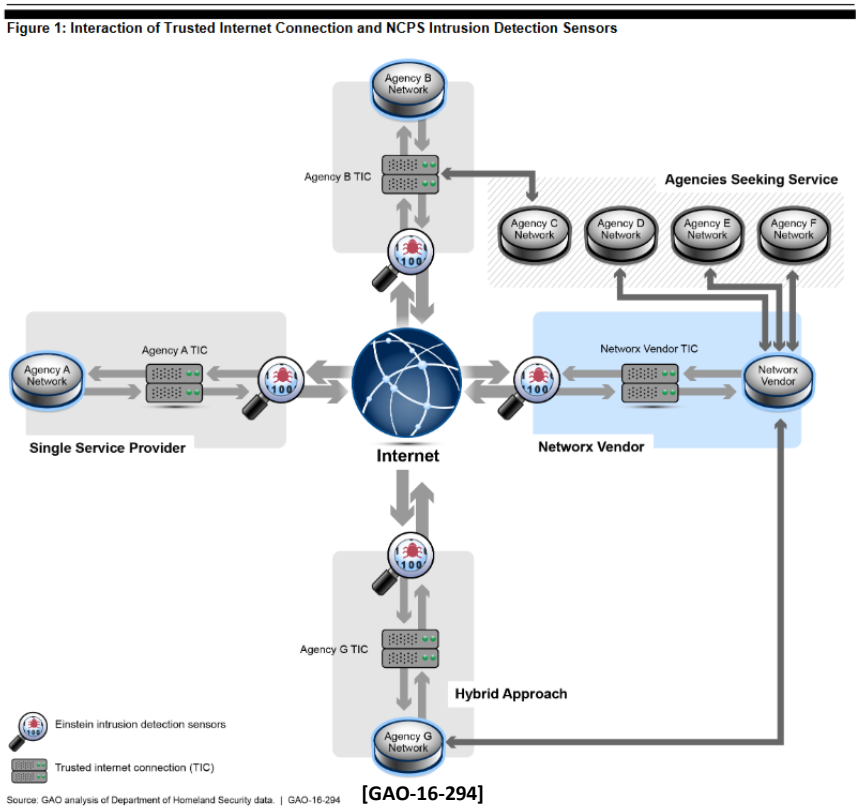
- Different tools may analyze the same source data
- Use of transparent middle-boxes for monitoring and mitigation
- Correlation occurs across “sites” and “protocol features”
- May be governed by Privacy Impact Assessments

Missions [GAO-16-294] [CJCSM-6510.B]

- Cross-organization visibility
- Targeted hunting and event mitigation
  - Data Loss Prevention
  - Intrusion Detection and Prevention
  - Incident Containment (Information Sharing)
- Incident Response

Exemplar: National Cyber Security Protection System (EINSTEIN)

EINSTEIN … is to augment -- not replace or reduce -- the current computer network security practices of participating federal executive agencies. Participating agencies will continue to operate their own intrusion detection and prevention systems, perform network monitoring, and use other information security technologies. EINSTEIN … enables the US-CERT to correlate activity across the entire federal enterprise. [EINSTEIN2-PIA]



Coming Changes of Interest

TLS v3 [PERVASIVE-CRYPTO]

- *Community Practice*: middle-boxes transparently terminating connections for inspection
- *IETF Background*: TLS (Transport Layer Security)
- *Future Work*: maintaining visibility with forward secrecy

Encrypted DNS [PERVASIVE-CRYPTO]

- *Community Practice:* passive DNS monitoring in enterprise and at gateways
- *IETF Background:* DPRIVE (DNS PRIVate Exchange) and DOH (DNS Over HTTPS)
- *Future Work*: maintaining visibility

MultiPath TCP [MULTIPATH-TCP]

- *Community Practice*: (asymmetric routing aside) inspection on single streams
- *IETF Background*: MPTCP (Multipath TCP)
- *Future Work*: evolving technology for multi-stream analysis

Evolutions in Operating Model

Temporary Loss Of Visibility

- Increased coordination between security operators

Changes in workflow

- Acquiring features through alternative (non-network) sources
- PaaS and SaaS migration will put all security operators on equal footing
- Increased use of behavioral profiling

References

[CJCSM-6510.B] Cyber Incident Handling Program. 2014. http://www.jcs.mil/Portals/36/Documents/Library/Manuals/m651001.pdf?ver=2016-02-05-175710-897

[DOD-CIO-CONSENT] Policy on Use of Department of Defense (DoD) Information Systems-Standard Consent Banner and User Agreement. 2008. http://dodcio.defense.gov/Portals/0/Documents/DoDBanner-9May2008-ocr.pdf

[EINSTEIN2-PIA] Privacy Impact Assessment of EINSTEIN 2. 2008

https://www.dhs.gov/publication/dhsnppdpia-008-einstein-2

[EINSTEIN3A-PIA] Privacy Impact Assessment of EINSTEIN 3 Accelerated. 2013.

https://www.dhs.gov/sites/default/files/publications/privacy/PIAs/PIA%20NPPD%20E3A%2020130419%20FINAL%20signed.pdf

[GAO-16-294] DHS Needs to Enhance Capabilities, Improve Planning, and Support Greater Adoption of Its National Cybersecurity Protection System. 2016. https://www.gao.gov/products/GAO-16-294

[MULTIPATH-TCP] Multipath TCP: Breaking today's network with tomorrow's protocols. 2014. https://www.blackhat.com/docs/us-14/materials/us-14-Pearce-Multipath-TCP-Breaking-Todays-Networks-With-Tomorrows-Protocols.pdf

[PERVASIVE-CRYPTO] Effects of Pervasive Encryption on Operators. 2018. https://datatracker.ietf.org/doc/draft-mm-wg-effect-encrypt/