Compliance: The Enterprise Vulnerability Roadmap

. . .

Weasel

Nomad Mobile Research Centre

weasel@nmrc.org

Introduction

The Semi-Security State of Compliance

- Overview of Compliance Benefits and Standards
- Things Compliance Gets Wrong
- Detrimental effects of Compliance
- Paths of Attack Provided by Compliancy

Compliance Benefits

- Old, hard-to-sell controls finally being implemented
- Standardization of common controls
- “Credentials” for lazy people who don’t want to work or go to school (OK, so that’s not a benefit…)

Compliance Standards

- COBIT: Control Objectives for Information and related Technology (ISACA)
  - Best Practices/Framework/Guidelines for IT Management
- PCI DSS: Payment Card Industry Data Security Standard (PCI)
  - Guidelines for processing, storing, and transmitting credit card data
- HIPAA: Health Insurance Portability and Accountability Act
  - Standards for the use and dissemination of health care information

Compliance Standards (Cont)

- GLBA: Gramm-Leach-Bliley Act
  - Mostly policy-centric guidelines for protecting the privacy of financial data
- SOX: Sarbanes-Oxley Act (SEC)
  - Financial data retention and integrity
- ISO/IEC 27000 Series, ISO 17799/BS7799-2:
- ITAF: Information Technology Assurance Framework (ISACA)

The Psychological Impact of Compliance on the Enterprise

- False Senses of Security
  - Primarily due to ignorance, stupidity, or vendor misrepresentation (see: “ignorance” and “stupidity”)
- Misinterpretations of concepts
  - Primarily Vendor-Fueled
  - Also fed by lack of education to decision-makers
- Budgetary and Resource Shifting and Mayhem
- The “Pass the Audit” vs. “Secure the Systems” Paradox
  - Security ~= Complaint, whereas Compliance != Security

Compliance is the Self-Devouring Serpent

- Misrepresented/Misinterpreted Postures
- Conflict of Interests
  - Auditors are paid for results (find something), but don’t want to lose business (don’t find too much)
- Governance Hypocrisies
  - Some governance organizations also make money through certifications and training
    - Primary motivation is continuity of business
- "Secure" vs. "Passing Audit" paradox
- Things you may not have known about compliance boards

The Anti-Progression Trap

- Compliancy can lock organizations into “old” technologies and architectures
  - Technology requirements where logically not needed or crippling
    - Requiring Firewalls where emerging concepts don’t call for one
  - “Anti-virus is Dead”

Notes on the "Risk Bandwagon"

- Definition
  - “We don’t understand it, so just manage the risk rather than mitigate.”
  - “Why spend $1M to mitigate a risk when managing it only costs $250k”
- A new mentality is evolving
  - Knowing the enemy before you know who it is

Compliance brings us a new fingerprinting foundation

- Standards == Defined Attack Matrix
  - Passwords: length, complexity, age, etc
  - Data Retention: Data is expected/known to exist
  - Policy: Chaos and Weakness
  - Configuration Management: Workstation, Server, Data Centers, Applications, Infrastructures

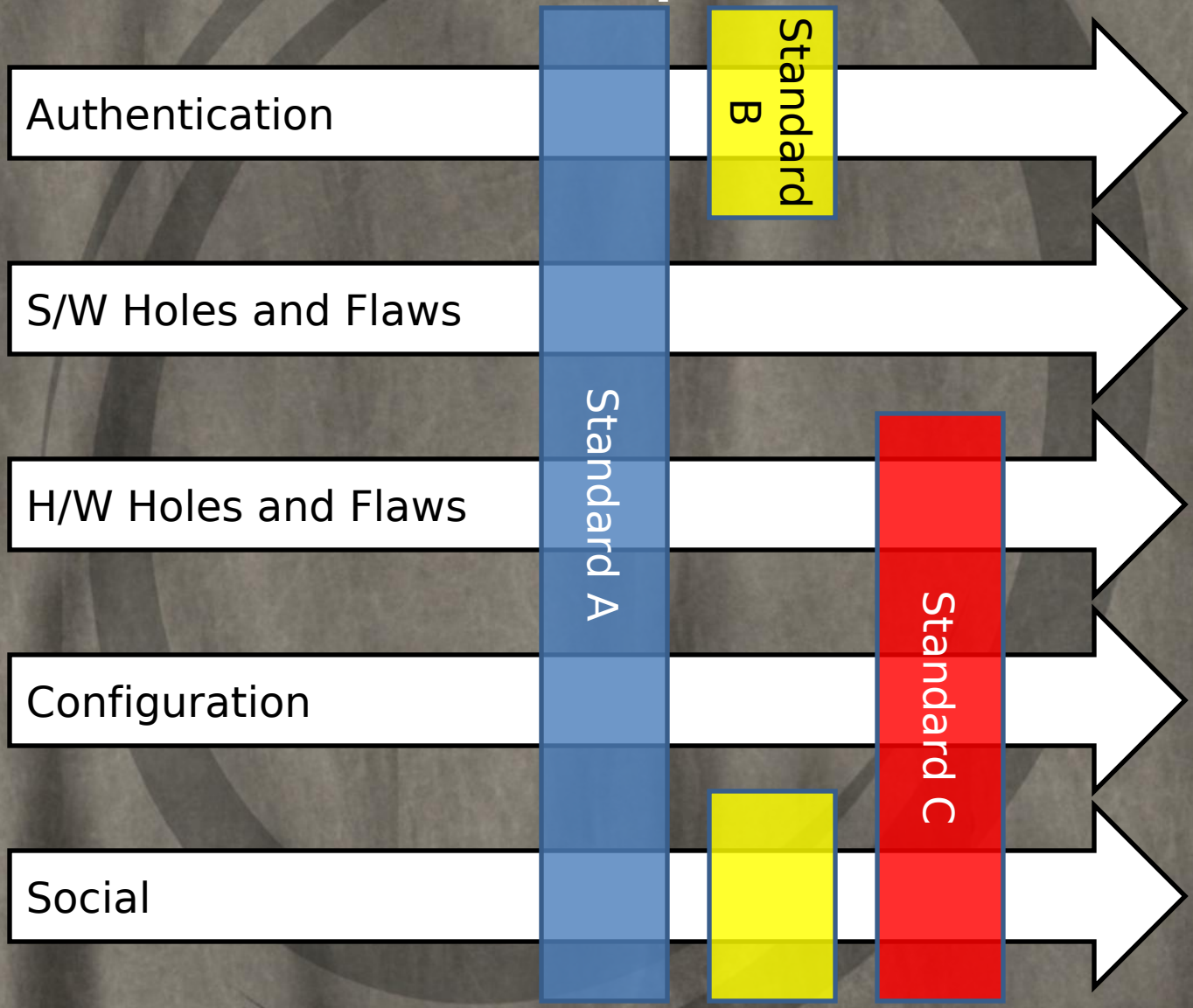
Other Standardizations

- Encryption requirements
  - standard algorithms
    - No time wasted forcing non-compliant algorithms
  - sensitive data flagging
    - Encryption flags the “juicy stuff”
  - Key management

Using Compliance to Map Penetration

- Know what compliancies govern the target
- Know what data exists before attack
  - Know what controls are in place to protect the data/system due to compliancy (because we know it's likely not to exceed the compliancy minimum)
- Set the attack tools to start at compliancy minimums (saving time and reducing detections)

Example


Authentication
S/W Holes and Flaws
H/W Holes and Flaws
Configuration
Social
Standard A
Standard B
Standard C

Tool Request

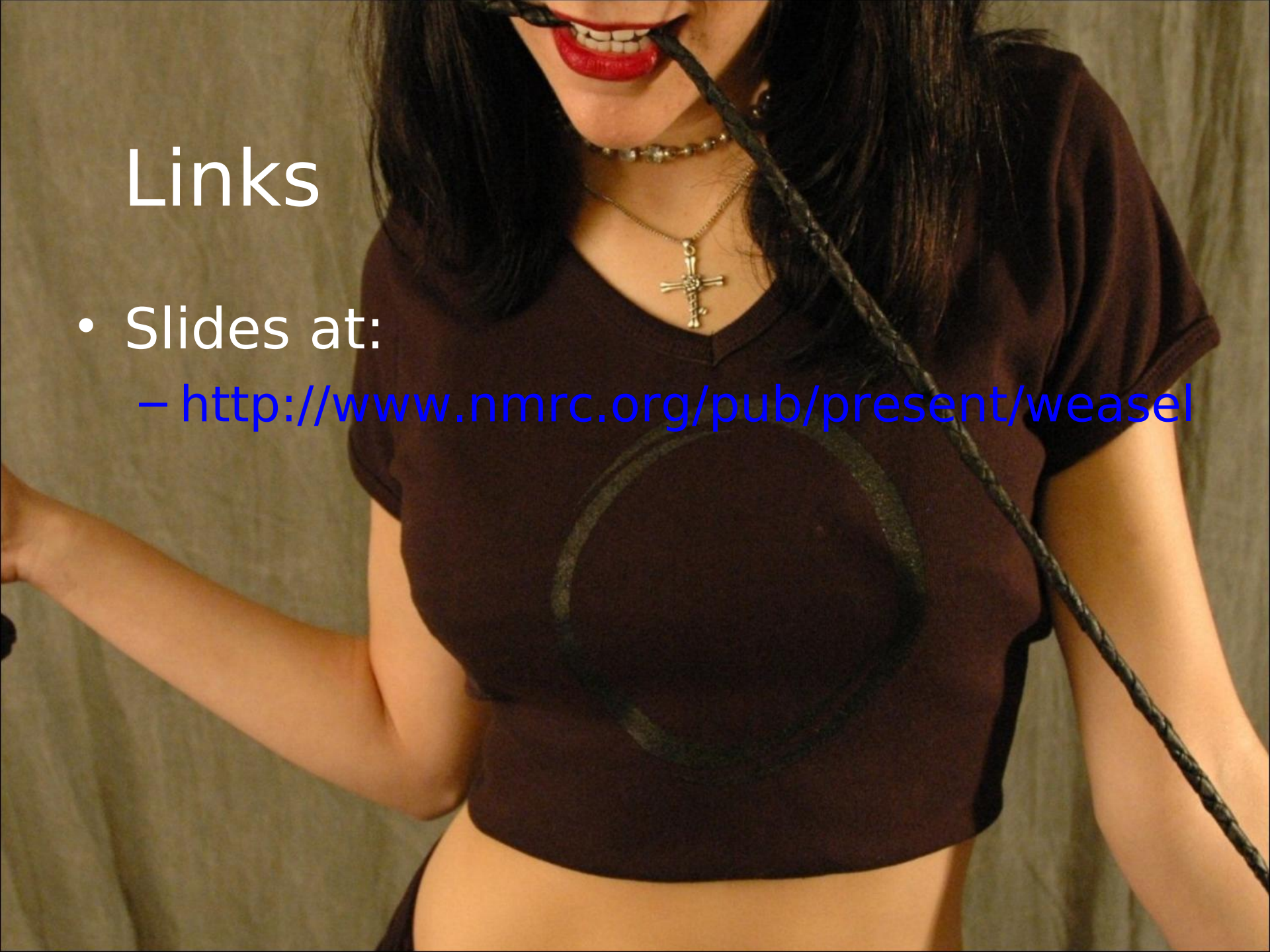
- Attack Matrix Tool
  - Target Attributes
    - Business Domain, Country, Public/Private etc
  - Display Attack Avenues
  - Output to tool formats
    - Nmap, Burp Suite, Etc
  - Output to environment formats
    - VM’s, Web Goats, etc

Conclusion

Q&A

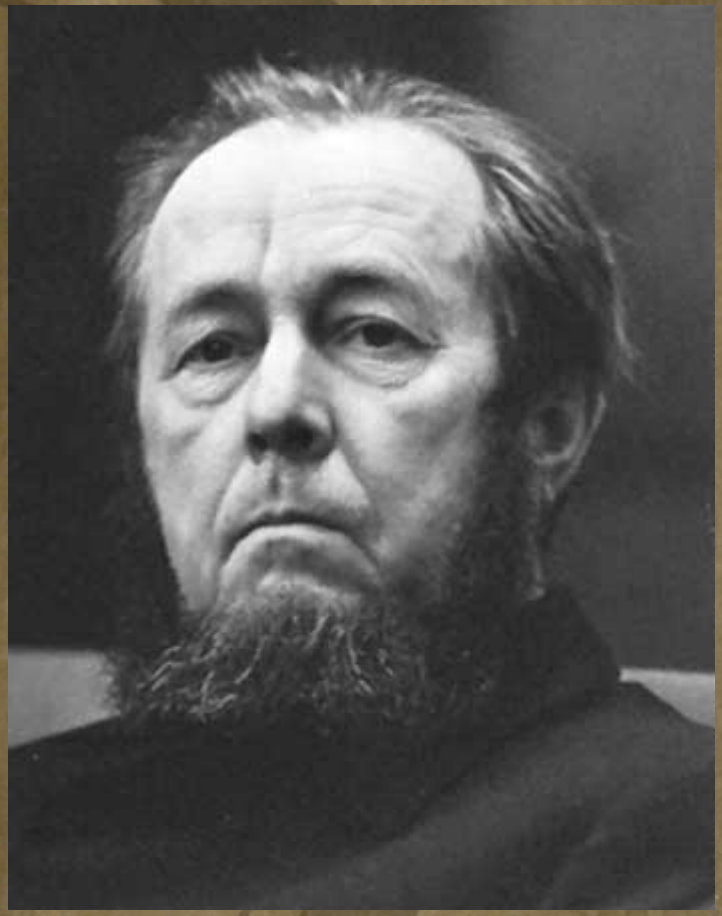
BlackHat 2008 Notes

- The “Room Security” Illusion
- The Gauntlet of Insanity
  - Wheel of Annoyance
    - Including Room Visits
  - Booth Babes



Links

- Slides at:
  - http://www.nmrc.org/pub/present/weasel



Aleksandr Solzhenitsyn

Dec 11, 1918 – Aug 3, 2008