Security Automation: The *Trail* Ahead

Tony Sager

Chief, Vulnerability Analysis & Operations Group

Information Assurance Directorate

National Security Agency

September 28-30, 2010

6th Annual IT Security Automation Conference

Lessons Learned

- The optimal place to solve a security problem is ...
- If it is happening to you today, then ...
- After you figure out what happened, there were ...
- So, the future of Cyberdefense is...

Lesson 1

The optimal place to solve a security problem is ...*never where you found it.*

--Corollary: the information for the solution is never in the right form for the solution

Lesson 2

If it is happening to you today, then ...

...*something very much like it happened to someone else yesterday, and will happen to someone else tomorrow***.**

--Corollary: and you probably don't know them

Lesson 3

After you figure out what happened, there were…*plenty of signs that *could* have helped us prevent or manage this*.

--Corollary: but not all the signs are in "cyberspace", or available to "cyber defenders"

So, the future of Cyberdefense is really about…

Information Management!

Visions of a cyber ecosystem

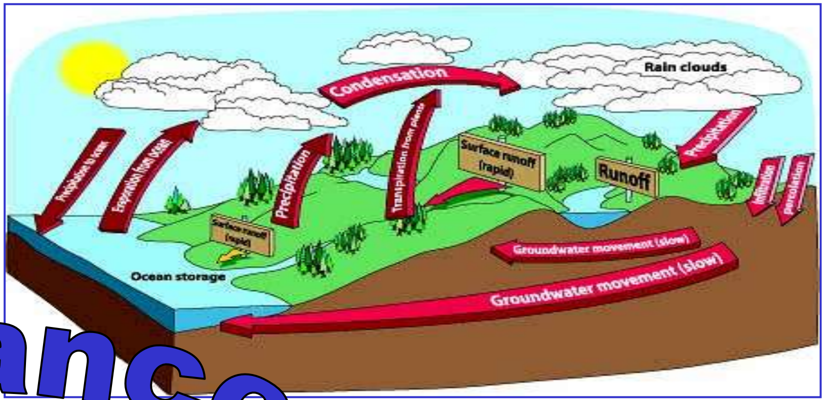
"Every computer in the DoD

is configured as securely as possible,

all of the time,

and the right people know that this is so

(or not so)."



assurance

- Automation
- Interoperability
- Authentication

"…separate the security content from the delivery mechanism…"

"…but the other end might lie to you…"

In a healthy ecosystem

we will ***not***…

- focus on devices, but on information
- distinguish btwn info created by humans and tech
- focus on categories like “security information”
- create singular repositories of information
- create info solely for/from discrete transactions
- buy stand-alone tools or information

In a healthy ecosystem

we will *__have__*…

- massive and rapid information “reach”
- new analytics (e.g., reachability, dependency)
- a way to assess the value of new information
- new defensive tactics (e.g., dynamics, uncertainty)
- new measures of confidence/assurance
- linkage from policy to implementation, and back
- global visibility based on local execution
- a “closed loop” of assurance

Automation Landscape

Security Content

- NIST Checklists
- NSA Guides
- DISA STIGs
- IT Mgmt Data
- Threat Reports
- Signatures,

indicators

- Ops Test Data

Standards Plumbing

- SCAP
- MAEC
- CWE
- CAPEC
- CEE
- ……

Capabilities

- Net Mgmt
- Scanners
- Patching
- Asset Mgmt
- Whitelisting

Use Cases

- Dept of State iPost
- DoD CND Data Sharing Pilot
- IC “Gold Standard”
- DoD Sensor Grid
- IA Campaign Plan

Public-Private Partnership

one government lifer's view

- ***The govt. must bring content to the table***
  - ***Delivered by great people…***
- ***Work with all stakeholders in parallel***
- ***Separate the content from the delivery mechanism***
- ***Act like a Partner***