The Office of the National Coordinator for Health Information Technology

Moving Security Beyond the Technical

Tales from the Research, Industry, and Government Trenches

Jeremy Maxwell, PhD
Office of the Chief Privacy Officer
Office of the National Coordinator for Health IT
US Department of Health and Human Services

About Me

- PhD computer science
  - » Research: Reasoning About Legal Text Evolution for Regulatory Compliance in Software Systems
- 5 years security architect @ leading EHR vendor
  - » Coordinated privacy, security, compliance
- 1.5 years @ ONC
  - » Senior technical advisor, security

Main Theme

To deal with security threats in 2016…

“Traditional” security advice won’t work

The way we approach security needs to be rethought

The Rest of the Talk

- Moving security beyond the technical in industry
- Moving security beyond the technical in research
- Moving security beyond the technical in healthcare

Security in 2016
Searching for the Right Metaphor

Metaphors Matter…

"Users are our worst enemy…"

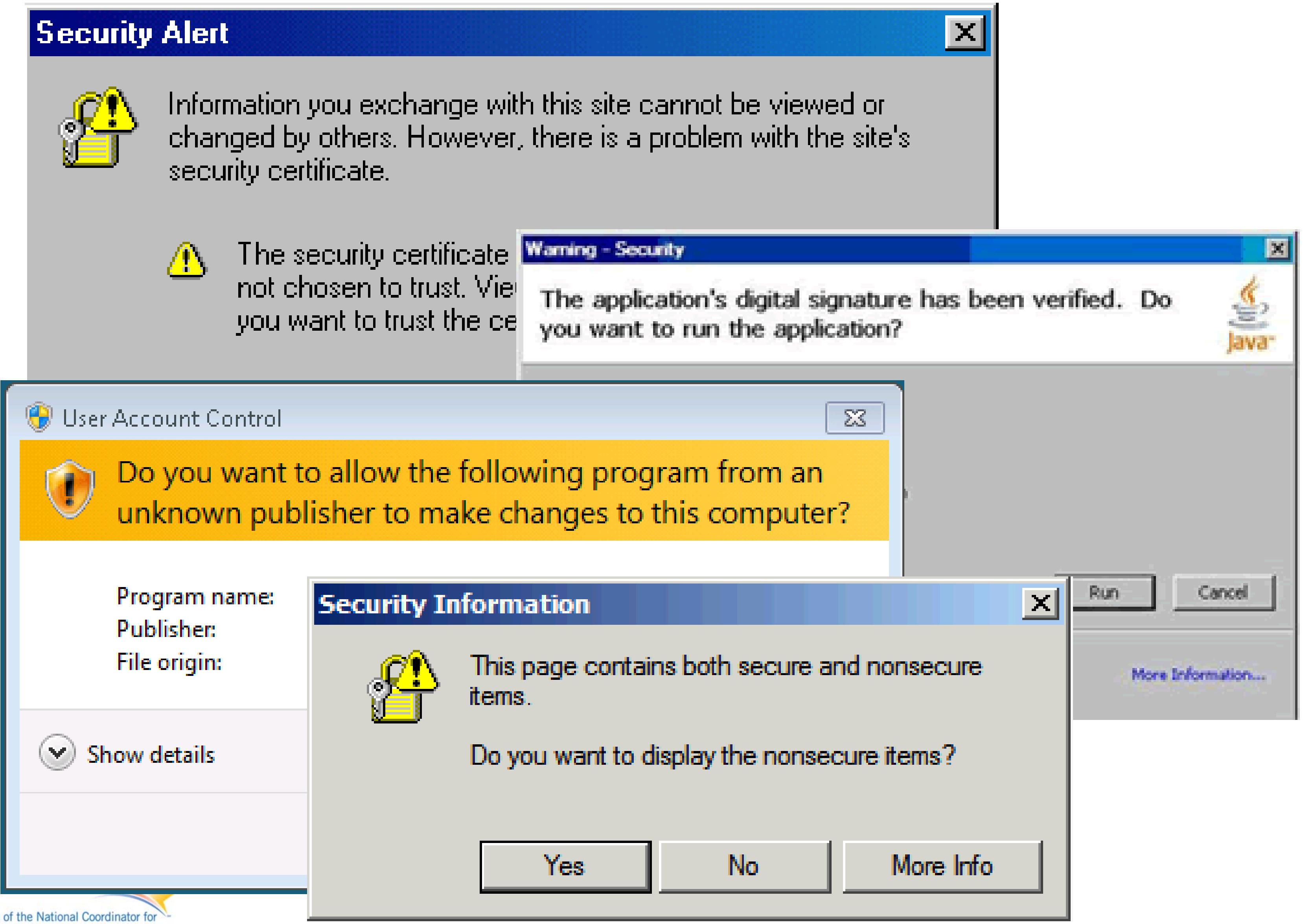
"Users are our weakest link…"

Shifting the Conversation

USTICE
RACY
NG
VESTIGATION
HOMELAND SECURITY
INVESTIGATIONS
U
S
SPECIAL AGENT

horized reproduction or
of this copyrighted work is
al copyright infringement is
by federal law enforcement
punishable by up to 5 years
and a fine of $250,000.

What Do All These Say?



Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

The security certificate
not chosen to trust. Vie
you want to trust the ce

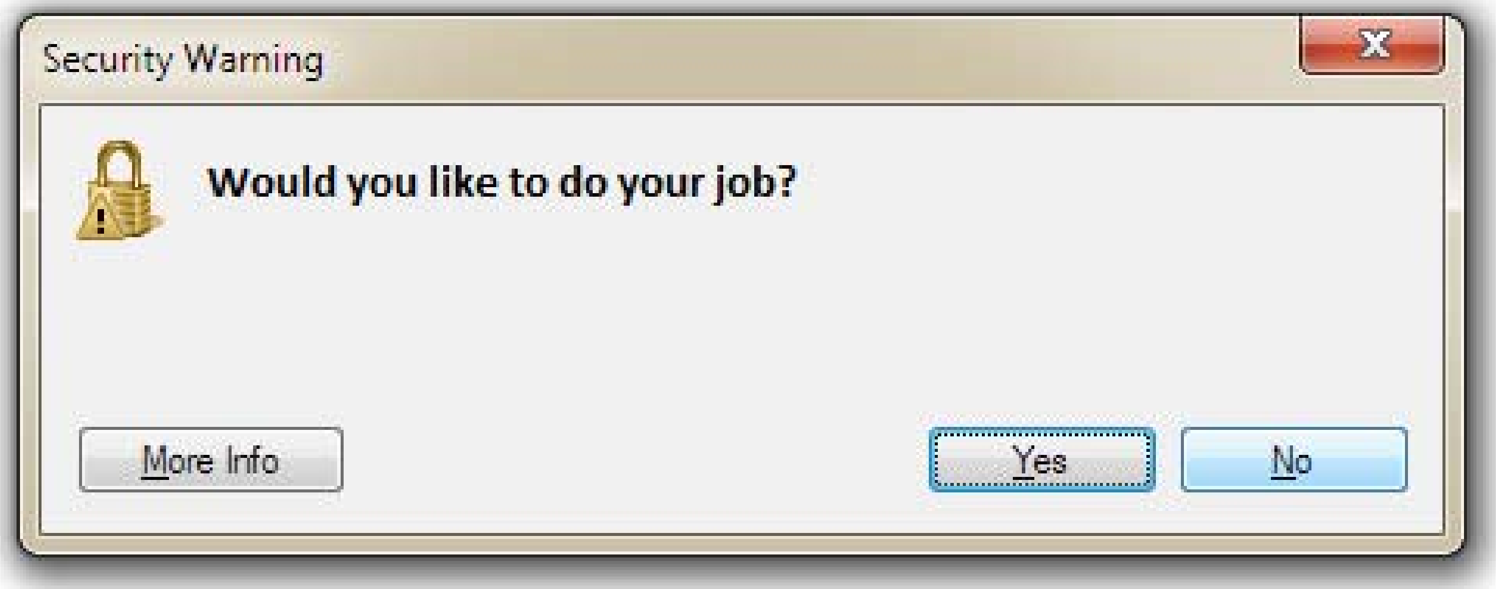
The application's digital signature has been verified. Do you want to run the application?

Do you want to allow the following program from an unknown publisher to make changes to this computer?

Program name:
Publisher:
File origin:

This page contains both secure and nonsecure items.

Do you want to display the nonsecure items?

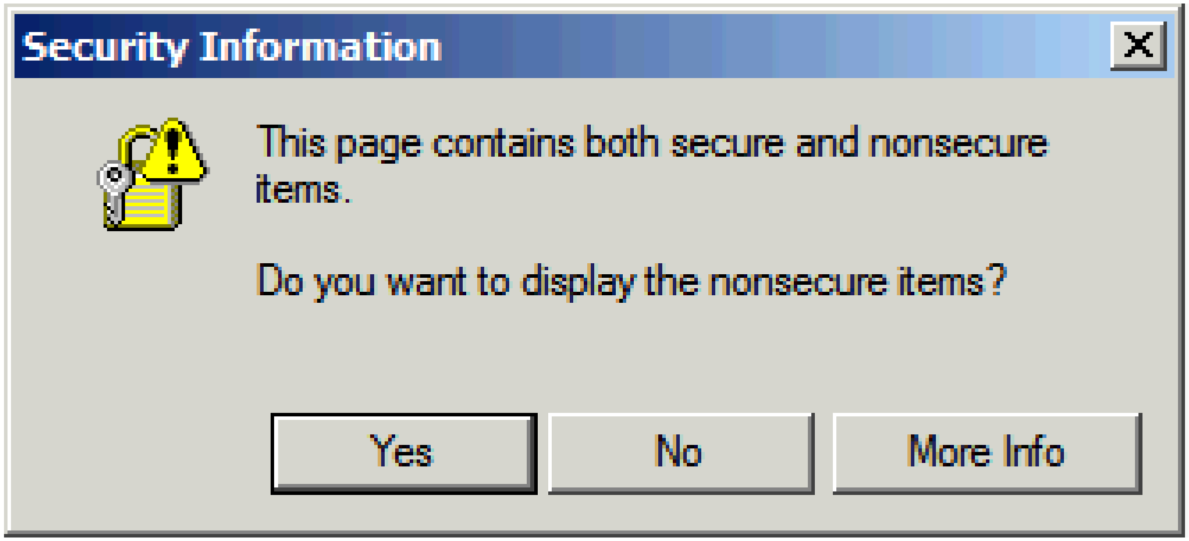


Security Warning

Would you like to do your job?

Security Needs More…User Centered Design (UCD)

- Secure system use should be easy…insecure system use should be hard
- Poor UX design leads to insecure system use



Security Information

This page contains both secure and nonsecure items.

Do you want to display the nonsecure items?

Security Needs More…Education

- Why aren’t awareness & training programs more effective?

- Phishing (Verizon 2016 Data Breach Investigations Report)
  - 30% of users open phishing emails
  - 12% of users open attachments

- Should we blame users who are victimized by phishing?

Security Needs More…Business Process Reengineering

Can you send me that file?

Sure, but it’s too big for email

No problem, just upload it to ________

Ok

- Focus should be on security as an enabler, not as a detriment to “getting stuff done”

- Business processes should be secure by default

Security Needs More…Historic Preservation

- What to do about poorly written code?
  - VB6
  - 10K line functions
  - Hundreds of edits by dozens of users
- In general, poorly written code is less secure code
- What about when that code is in safety critical functions and have been stable and bug free for years?
- We need degrees in historic software preservation
  - Knowledge transfer
  - Vendor end-of-life
  - Open source lifecycle management

Security Needs More…Applied Psychology

- Phishing uses Machiavellian techniques to con victims into surrendering data, credentials, or downloading ransomware

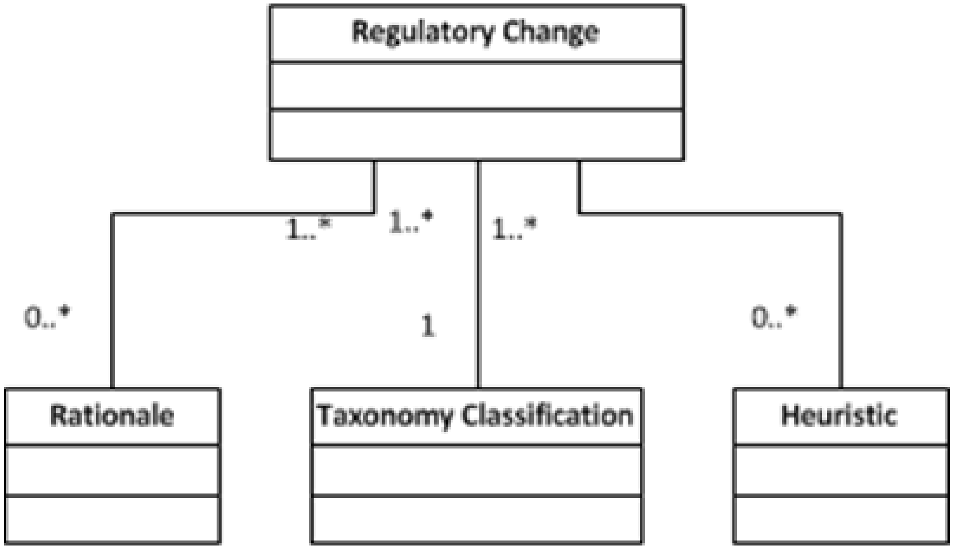
- Apply the same psychological techniques used to study con artists
  - » Apply to phishing with kill chain analysis

Enough about Phishing…

- Moving security beyond the technical in industry
- Moving security beyond the technical in research
- Moving security beyond the technical in healthcare

How Do You Managing Changing Compliance Requirements?

- 2012: Developed an adaptability framework for managing changing compliance requirements [MAS12]



Predictive Heuristics [MAS12]

H_1: Ambiguous req’ts may be disambiguated.

H_2: Repeated concepts may be formally defined.

H_3: Duplicative concepts may be combined or disambiguated.

H_4: Technology-specific requirements may be removed.

H_5: Specific req’ts subsumed by a broader req’t may be removed.

- Given a proposed rule, helps engineers identify which areas are likely to change
- Only predict *that* a section of the rule will change, not *how*
  - No 1-to-1 mapping exists

Security Needs More…Political Science

- Summative Study Results [MAS12]

	Accurate	Inaccurate
Predicted	11 (true positives)	5 (false positives)
Not Predicted	104 (true negatives)	33 (false negatives)

Accuracy (the ratio of predictions that were correct)	0.75
Precision (the ratio of predictions that were accurate)	0.64
Recall (the ratio of the regulatory changes we identified)	0.21

- True positive – changes that we accurately predicted
- False positive – changes we predicted that were not accurate
- True negative – a legal statement for which we predicted no change and for which no change occurred
- False negative – a legal statements for which we predicted no change and which changed in the final rule

Enough about Adaptability…

- Moving security beyond the technical in industry

- Moving security beyond the technical in research

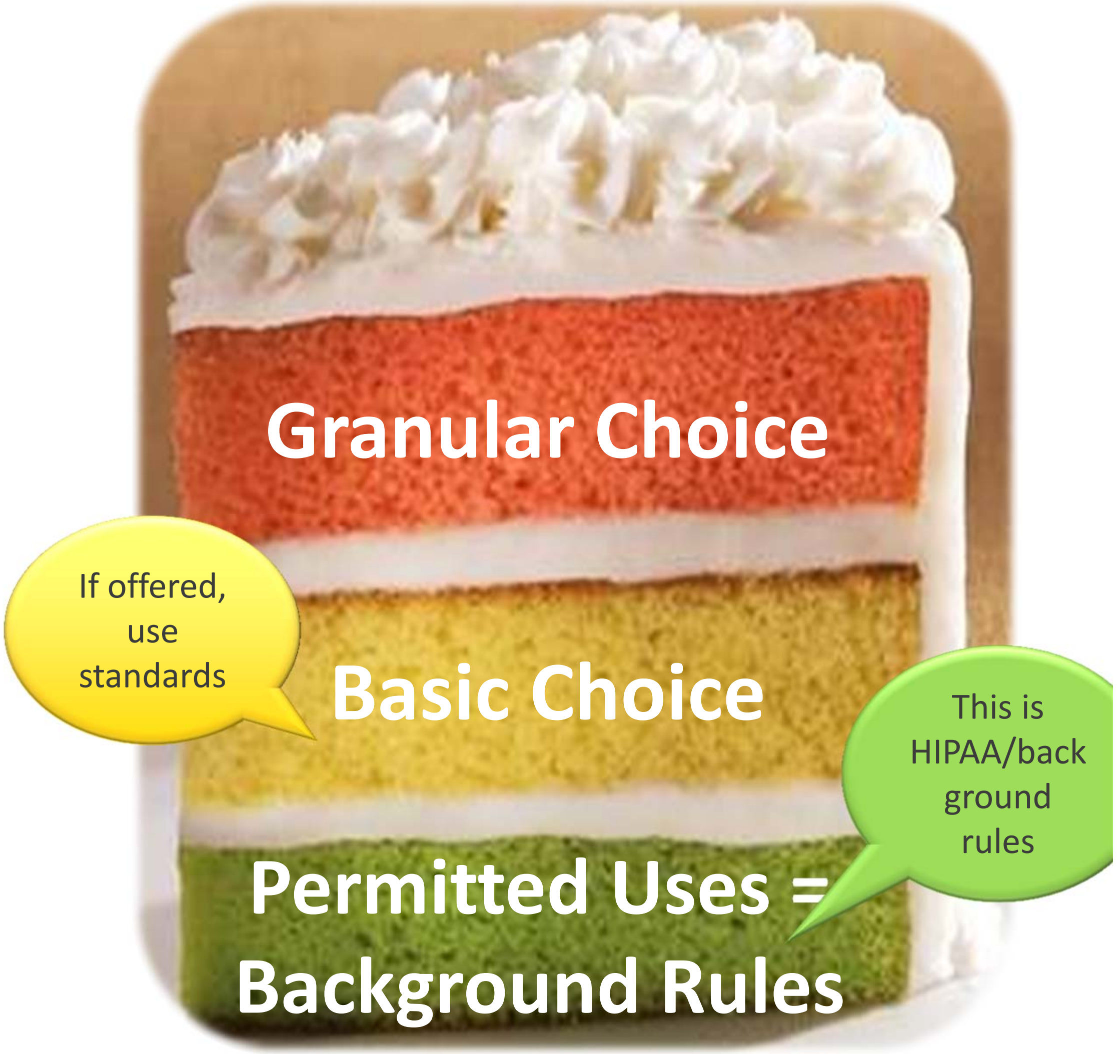
- Moving security beyond the technical in healthcare

Precision Medicine Initiative

- Announced in January 2015
- Goal is to accelerate biomedical discoveries and provide clinicians with new tools, knowledge, and therapies to select which treatments will work best for which patients.
- One of the challenges is managing consent (access control)

Three Levels of Rules All Must Be Computable

- **HIPAA runs in the background** and permits disclosure for health
- **Basic Choice** refers to the choice an individual makes about the use and disclosure of health information, including the electronic exchange of health information, irrespective of default rules.
- **Granular Choice** is the choice an individual makes regarding the distinctions between legally sensitive clinical conditions, such as mental health or HIV/AIDS status and evolves over time to enable choice about disclosure to specifically identified participants in the health care system.


Granular Choice
If offered, use standards
Basic Choice
This is HIPAA/back ground rules
Permitted Uses = Background Rules

The Office of the National Coordinator for Health Information Technology

DS4P Standards: What can DS4P do?

- Data Segmentation for Privacy (DS4P) is a technical standard that specifies how to “tag” clinical data with privacy metadata to express confidentiality levels and downstream obligations
- Segmentation can occur at the document or field level
- Balloted as a normative standard under HL7
- HIT developers can certify for DS4P under the ONC 2015 Edition Certification Rule

Policy Challenges

Laws tell data-holders not to disclose; law rarely tells them what to say about that non-disclosure. For example:

HIV Status: **Redacted**

This is a likely indicator that the patient has a test result

if the applicable law protects results of tests, not occurrences, this may indicate a positive result; or

HIV Status: **No data available**

This is may be misleading for a physician, who may then make a health decision for the patient without knowing important details that could lead to safety issues.

HIV Status: **[record is silent]**

This is ambiguous. The recipient does not know if there was a redaction, or no data is available.

Data Segmentation: Things to Solve

- **How to Segment:** There are multiple levels at which segmentation could occur, such as:
  - Type of Data category of data - e.g. medications, diagnostic codes, etc.
  - Clinical category of code of whatever type
  - Disclosing provider
  - Intended recipient
  - Facility type (e.g. Part 2 clinic)

- **Structured vs unstructured Data:** Prevalence of free-text complicates identification of data that is subject to enhanced protection.

Data Segmentation: Things to Solve

- **Granularity:** Should data be segmented:
  - » At the "whole document" level?
  - » For parts of a document?
  - » According to clinical nature within the document?
- Standardized mapping of specially protected categories to codes would make segmentation more predictable:
  - » For individuals through standard understanding
  - » For providers through standard expectations
  - » For developers, with less confusion about what law requires
- Currently, not every receiving system can understand 42 CFR Part 2 segmented data, i.e., their system does not recognize that it is receiving data that is subject to heightened protections based on Part 2 law.

Security Needs More…Game Theory

- Patients must make decisions to segment data based on imperfect information
- Clinicians must make clinical decisions based on imperfect information
- PMI participants must make consent decisions based on imperfect information

Access control systems are binary

Wrapping It Up…

Main Theme

To deal with security threats in 2016…

“Traditional” security advice won’t work

The way we approach security needs to be rethought

Q & A