ANAKAM
ONLINE SECURITY SOLUTIONS

Accelerating HIT adoption by combating online fraud

Safety in CyberSpace
Segue from Financial Services to Healthcare

Confidentiality, Privacy & Security Workgroup

September 29, 2006

ANAKAM LLC 888-826-2526 / 858-622-9584 Fax
5665 Oberlin Drive, Ste 106, San Diego, CA 92121

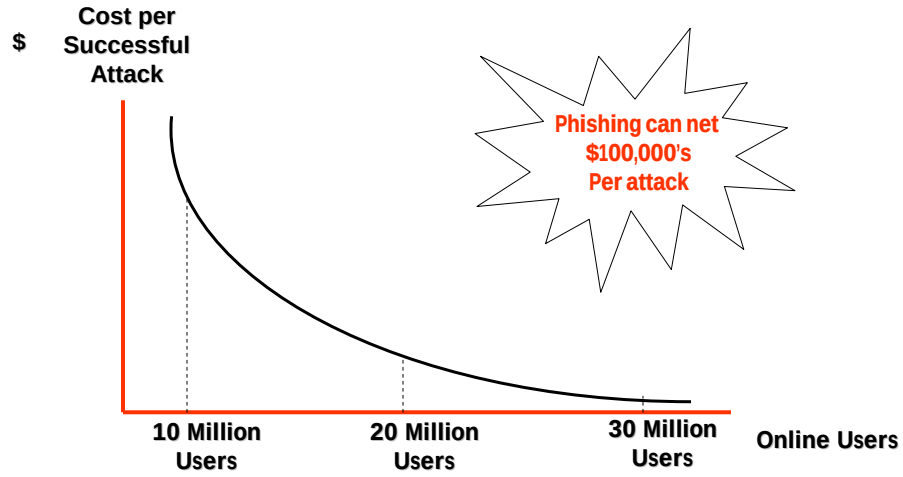
We have seen the future…it is online financial services

- Five hundred Phishing and other online attacks per day
- Massive consumer fear and lack of adoption due to privacy concerns
- NIST E-Authentication guidelines and FFIEC Guidance (for financial institutions) clearly state that single factor (user name and password) is not adequate security
- Banks across the country are rushing to adopt second factor authentication to secure their consumer facing portals and protect their brands

FORE
Foundation of Research and Education of AHIMA

"Healthcare needs to follow the example of on-line financial services industry"

Fraudsters often times strike web sites with the largest user bases…where they can achieve economies of scale



Lessons Learned from the Financial Services Industry

- Financial services industry able to "tolerate" a certain amount of fraud
- Whereas a breech of patient's substance abuse, mental health or HIV status represents a much larger risk to users, public trust and system owner brand equity
- Banking has slowly evolved with greater levels of security as the sophistication of attacks has increased…unfortunately always a reactionary response:
  - User name and password>>high entropy passwords and extra PINS>> institutional questions>>two factor authentication
- Realization that hard token devices too expensive and logistically cumbersome to distribute to very large populations of remote users
- Differential levels of security for high net worth customer groups poorly received by overall customer base…all customers deserving of security
- Low touch or no touch ID proofing have been successful and worthy of emulation in healthcare industry
- Federal policy guidance needs to be detailed, clear and explicit to drive industry adoption. Vague guidance can lead to industry frustration and poor implementation

Multi-Layered Defense: Binding the ID Proofing Transaction with Credentialing and the Authentication Transaction

- **First component, Registration, provides necessary info to complete the ID proofing and credentialing transaction**
- **Second component, ID proofing, verifies authenticity of the claim of identity, generally a one time event**
  - **In person ID proofing more difficult but can be effective if executed well**
  - **No touch electronic ID proofing systems can be equally effective is designed and implemented correctly**
- **Third component, Credentialing, defines attributes of the individual that will define how one's enterprise will work with them, may be a periodic event**
- **Fourth component, Authentication, binds the ID and credentials to the individual attempting to conduct a transaction through the use of**
  - **Something you know- a user name and password**
  - **Something you have- a hard token, usb device, cell phone, etc.**
- **Fifth component, Authorization and Access Control, critical for PHR's as patients and practitioners designate rights to access certain elements of the PHR**
- **Each of the components are complementary and reinforcing. A hacker may break one component but the other components will help minimize any potential breech of personal health information**

The role of Government in driving policy for identity proofing and authentication

- Government in concert with industry should establish minimum standards for ID proofing, credentialing, authentication and access control
- Privacy and security of personal health information justifies a minimum of Level 3 controls as defined by NIST SP 800-63
- Tie security levels to the roles of users within the PHR community versus the technical means to achieve the levels
- Clear standards and explicit policy guidance will help prevent some of the confusion and reactionary mindset that has hindered the financial industry's ability to implement appropriate ID proofing and authentication systems for combating online fraud

Potential implementation costs of ID proofing and authentication

- Software based solutions, which leverage ubiquitous hardware and require no software downloads for the end user are 80-90% cheaper than hard token solutions
- Interesting paradox…spending for PHR security actually saves money, here's how:
  - Increased security spending for ID proofing and second factor authentication leads to…
  - PHR systems that can safely store richer patient content and provide secure access for greater physician adoption…
  - Better content and more physician participation leads to better PHR usability and higher levels of patient trust…
  - Higher usability and patient trust drives greater user adoption rates…
  - Greater user adoption rates leads to lower costs per user and the ability to charge higher user fees
  - Higher fees and lower costs leads to increased profitability which more than offsets the initial cost of increased security spending for ID proofing and second factor authentication

- 7

Characteristics of a good ID proofing and authentication system for PHR's and EHR's

- **Be based on detailed standards jointly developed by government and industry.**
- **Allow no touch ID proofing upon enrollment**
- **Allow electronic credentialing of physicians and other medical practitioners using only the most trusted credentialing data sources**
- **Require second factor authentication that can be repeated within an application for added security while accessing the most sensitive areas within a PHR or EHR.**
- **Provide a real time fraud alert to patients and practitioners should a fraudster be trying to access a PHR or EHR.**
- **Be scalable and affordable by using hardware that is ubiquitous in the health care environment.**
- **Rely on an easy and intuitive user interface and require no software downloads for patients or practitioners.**
- **Provide technical non-repudiation, data integrity and customizable reporting for HIPAA/CLIA and other regulatory compliance requirements.**

The bottom line…

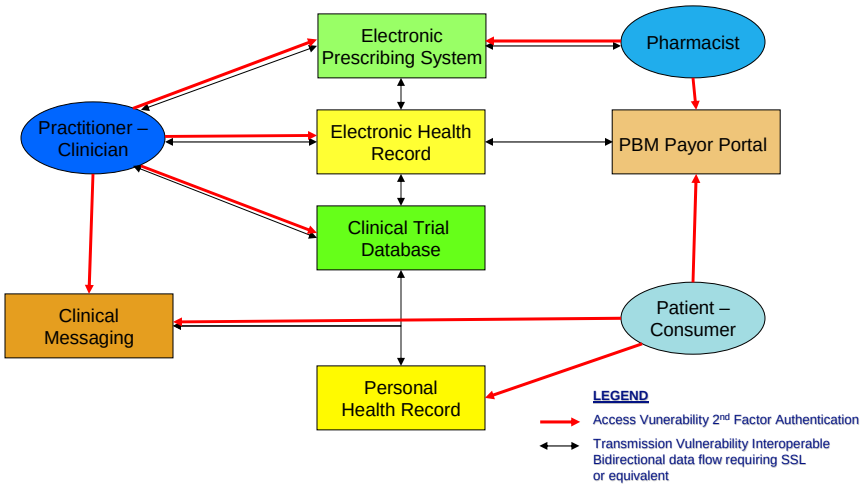
Working together, we all can contribute to developing a PHR which contains:

- Comprehensive patient information
- Available 24/7 to patients
- Fully endorsed by physicians
- Linked to resources relevant to patient needs
- Secured by an identity management system which fully protects the most important element of all: public trust

Index of Supplementary Slides

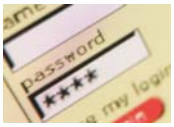
- "Points of Vulnerability for ID proofing and Authentication"
- "Second factor authentication primer"
- NIST: "OMB Memo M-04-04/NIST SP800-63: Recommendation for Electronic Authentication"
- NIST: "NIST Recognizes One-time Password Devices for Assurance Level 3"
- NIST: *"Cell phones could be good One-time Password Device Platform"*

Points of Vulnerability: ID Management - Authentication Assessment for Health Information Technology Universe



ANAKAM | ONLINE SECURITY SOLUTIONS

Second Factor Authentication Primer



- First or Single Factor Authentication
  - Something you know: I.D./password
- Second Factor Authentication for Online Applications
  - Something you have: Hard token, soft token, one-time password device, etc.
- Similar to an Automated Teller Machine (ATM)
  - Something you know: Password
  - Something you have: Debit card

- Second Factor Authentication is an effective mechanism to provide assurance of the identity of a person conducting an electronic transaction.

OMB Memo M-04-04/NIST SP800-63: Recommendation for Electronic Authentication

Assurance Levels

- OMB guidance defines 4 assurance levels
  - Level 1 little or no confidence in asserted identity's validity
  - Level 2: Some confidence in asserted identity's validity
  - Level 3: High confidence in asserted identity's validity
  - Level 4: Very high confidence in asserted identity's validity
- Needed assurance level determined *for each type of transaction* by the risks and consequences of authentication error with respect to:
  - Inconvenience, distress & damage to reputation
  - Financial loss
  - Harm to agency programs or reputation
  - Civil or criminal violations
  - Personal safety

NIST National Institute of Standards and Technology

NIST Recognizes One-time Password Devices for Assurance Level 3

Token Type by Level

	Assurance Level			
Allowed Token Types	1	2	3	4
Hard crypto token	√	√	√	√
Soft crypto token	√	√	√	
Zero knowledge password	√	√	√	
One-time Password Device	√	√	√	
Strong password	√	√		
PIN	√			

NIST National Institute of Standards and Technology

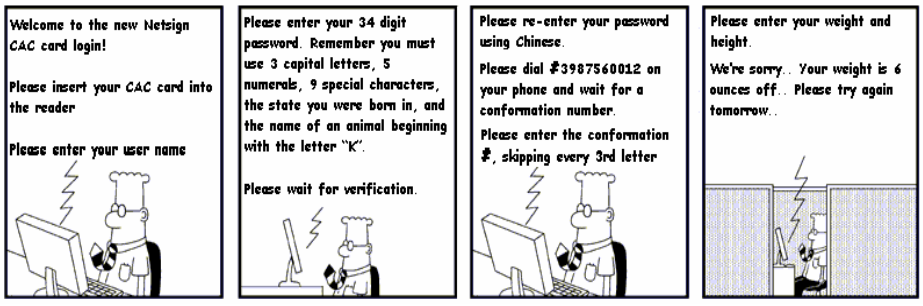
NIST: *"Cell phones could be good One-time Password Device Platform"*

PKI & E-Auth

- PKI solutions widely available
  - Can use TLS with client certs. for levels 3 & 4
- May be the predominant solution for levels 3 & 4 in gov.
  - Federal Identity Credentialing Committee
  - Common Credential and Federal Identity Card
    - Common certificate policy and shared service providers
    - Gov. Smart Card Interoperability Standard (GSC-IS)
- Fed. Bridge CA and Fed. Policy Authority are PKI vehicle
- Non-PKI level 3 & 4 solutions
  - One-time password devices in common use – can meet level 3
    - Cell phones could be a good 1TPD platform
  - Zero knowledge passwords for level 3 – not widely implemented
  - Level 4 could be done with symmetric key tokens

NIST National Institute of Standards and Technology

Identity Proofing and Authentication Systems Should Not Be A Barrier To Adoption



Questions?

John Macaulay
VP of Healthcare and Life Sciences,
jmacaulay@anakam.com

Anakam, LLC
(858) 622-9550