ARE MORE BROADLY USED AND TRUSTED IDENTITY CREDENTIALS ON THE HORIZON? YES!

Roger M. Callahan
Information Assurance Advisory, LLC
Password Exploitation

- Phishing
- Keylogging
- Guessing
  - Brute-force
  - Bulk Guessing
- Special Knowledge or Access Attacks
  - Guessing based on knowledge about the user
  - Shoulder Surfing
  - Console Access

Source: Dinel Florencio, Cormac Herley, Microsoft; Baris Coskun, Polytechnic University, Brooklyn, NY; “Do Strong Web-Passwords Accomplish Anything?” 2007
Password Exploitation

✓ Phishing
✓ Keylogging

- Guessing
  - Brute-force
  - Bulk Guessing

- Special Knowledge or Access Attacks
  - Guessing based on knowledge about the user
  - Shoulder Surfing
  - Console Access

Source: Dinel Florencio, Cormac Herley, Microsoft; Baris Coskun, Polytechnic University, Brooklyn, NY; “Do Strong Web-Passwords Accomplish Anything?” 2007
Account Hijacking of Corporate Customers

- NACHA, FS-ISAC and FBI in August 24, 2009 issued a joint paper with recommendations for customer education.

- It stated:
  - “In the past 6 months financial institutions, security companies, the media and law enforcement agencies are all reporting a significant increase in funds transfer fraud involving the exploitation of valid online banking credentials belonging to small and medium sized businesses.”
Malware Exploitation

- Manhattan U.S. Attorneys Announcement on September 30, 2010

  - 37 defendants charged with involvement in global bank fraud schemes.
  
  - The Zeus Trojan used to obtain account numbers, passwords and other vital security codes as they logged into their bank accounts online.
The previously referenced financial industry paper and a financial institution’s FAQ suggestion

- **How can I protect myself from being phished or acquiring malware?**

  “One of the best precautions you can take is to do all your online banking on a stand-alone, hardened, and completely locked-down computer on which no one can use email or browse the web.”
Some Movement Away from Fixed Passwords

One Time Password (OTP)

Token or Card Based

SMS Message
Zeus in Mobile Form Targets European Mobile Banking *

25 September 2010

S21sec Sean Sullivan blog reports:

“Zeus Mitmo: Man in the mobile (I)”

* eWeekEurope article, 29 September 2010, by Brian Prince
Government: (include)
- Open identity for Open Government
- E-Authentication Initiative
- National Strategy for Trusted Identities in Cyberspace (NS-TIC)
Strong Identity Proofing and Trusted Credentials

- Private Sector Collaborations (include)
  - Open Id Foundation
  - Organization for Advancement of Structured Information Standards (OASIS)
    - Identity in the Cloud (IDCloud) Technical Committee formed May 2010
  - Kantara Initiative
    - Identity Assurance WG
Financial Services Sector

- Issued an RFI for Improved Identity Proofing through a proposed research effort performed in collaborative manner with U.S. Government.
Strong Identity Proofing and Trusted Credentials

- Healthcare
  - National Health Information Network (NHIN)
    - Under Department of Health and Human Services
    - HIT Policy Committee Authentication Hearing held January 2010 to address planning.
    - October 15, 2010: Privacy and Security Team discuss “Provider Authentication for Health Information Exchange”
Obstacles to Overcome

- Trust
- Assurance
- Ubiquitous Interface
- Reach
- Cost
- Liability
How You Can Help

- Evaluate how you can contribute to advancing development and implementation of more broadly used and trusted identity credentials.
- Identify an effort that your organization or you can support or affect.
- Advocate for solutions with broad application.
- Assume an un-trusted platform will process the credential.
  - Advocate for cryptographic ancillary trusted hardware solution biometrically activated.
- Checkout activity on biometric thumb drives.
In Conclusion

THIS COULD HELP YOU TO AVOID ...

BIOMETRICS ARE THE FUTURE

Where did my money go?