



Biometrics and Access Token Technology, 10 Years Later...

Michael F. Angelo, CRISC, CISSP
NetIQ Corporation
angelom@netiq.com

Ron LaPedis, CISSP-ISSAP, ISSMP
Seacliff Partners International, LLC
rlapedis@seacliffpartners.com

Session ID: STAR-204

Session Classification: Intermediate

RSACONFERENCE2012

Genesis

- First presented
 - ~10 years ago (original was in 2000 to 2002)
- With all the incidents in 2011
 - Tons of Fear Uncertainty and Doubt
- Compare and contrast then and now



Agenda

- Basics
- Biometrics / Tokens
 - Changes
 - Deployment
 - Open Issues
 - Attacks
- Wrap-up, Conclusions, and Action Items



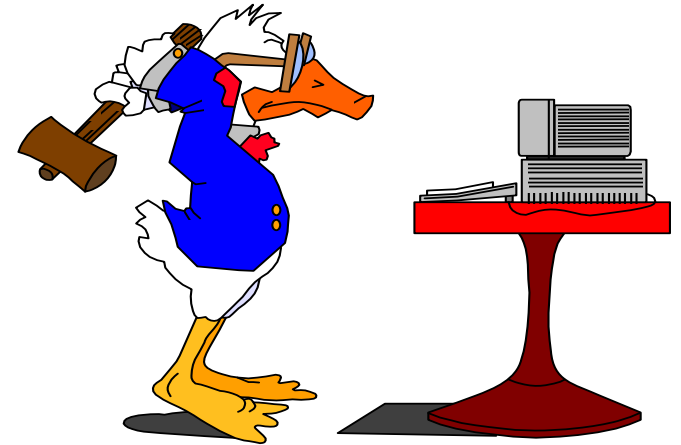
Basics

Proof of identity

Something you know: Password

Something you have: Token

Something you are: Biometrics



- Past
 - Fast and easy login for end users
 - Eliminates management of forgotten and expiring passwords (TCO reduction)
- Today
 - Still having problems



Does it Still Save Money???

- 2000 - User IDs & passwords are cumbersome
 - 50% help desk calls are password related
 - \$35 U.S.
- 2004 to 2010
 - 25% and 40% of calls (Forester / Gartner)
 - \$20 ~ \$30 per call
- Today:
 - Realization: Deployment infrastructure costs

Still NEED to Improve





Technology on Parade

Biometrics: Signature



Old

- Simple Capture
- Pen
- Rudimentary Timing

New

- Capture Ink & Motion
- Intelligent Pen
- Screens – cell phones
- Time, Motion, Pressure



Biometrics: Signature

- Deployment
 - Most stores (US) as part of Credit Card Sales
- Outstanding Issues
 - What do they match it to???
 - What happens with the signature image???
- Attacks
 - Figure out what they are doing
 - Get signature image



Biometrics: Fingerprint



Old



New

- Optical
- Solid State
 - Touch / Swipe
 - Cap / Thermal
- Lower Resolution
 - 300+dpi

- Swipe
- Touch
- Optical
- Higher Resolution
 - 500 + dpi

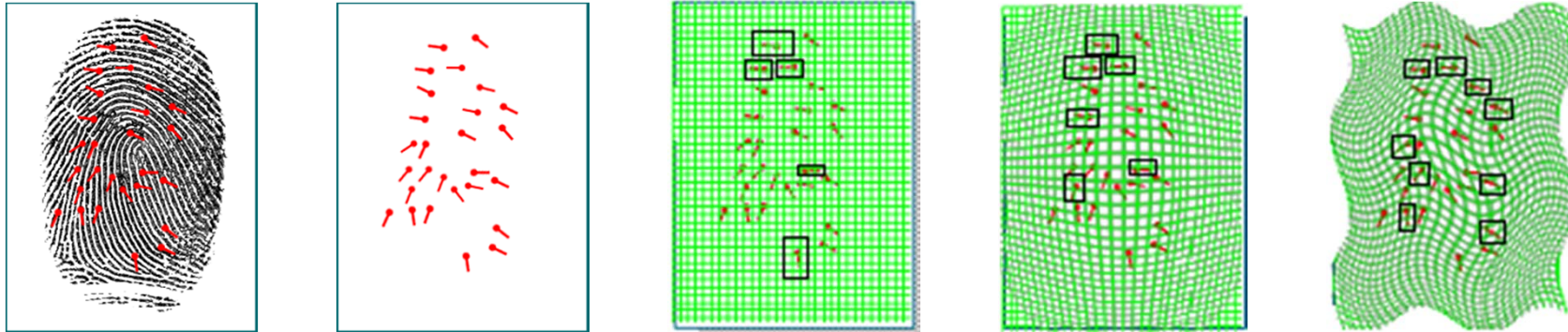


Biometrics: Fingerprint

- Deployment:
 - Country Level
 - Exit / Entry Programs
 - National Registration
 - Law Enforcement
 - Corporations
 - Local Login
 - Time and Attendance
- Outstanding Issues:
 - Optical Reader Issues haven't changed



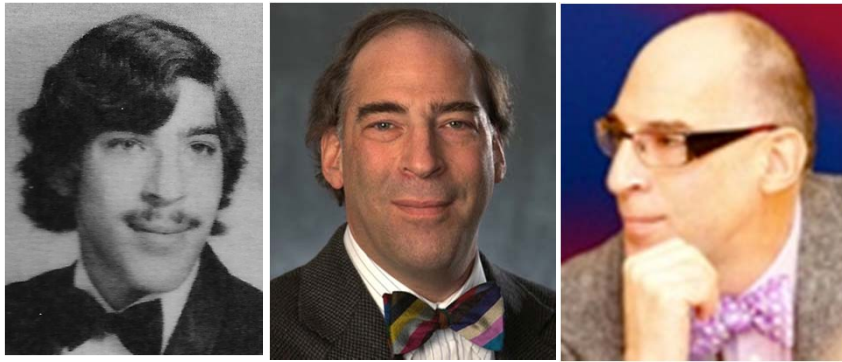
Biometrics: Fingerprint



- Latent Image
 - Direct Replay – use image on fingerprint reader
 - Duplicate Replay – get fingerprint & make a physical image
- Grid Attack?
 - Swipe prevents this? Right Well....
 - Make grid and then cast in rubber



Biometrics: Face (Single)



Old

- Low Resolution
- Cost \$\$\$



New

- Most HD or >
- Cheap
- Face Location
- IR / UV Illumination
- Composite



Biometrics: Face (Crowd)



- Government Use of Cameras
 - Identification of individuals out of a crowd
 - Law Enforcement
 - Exit Entry programs
- Outstanding Issues
 - Face Recognition and Facebook Tagging



Biometrics: Voice



Old

- Voice Capture
 - Limited words
 - Quality of Microphone

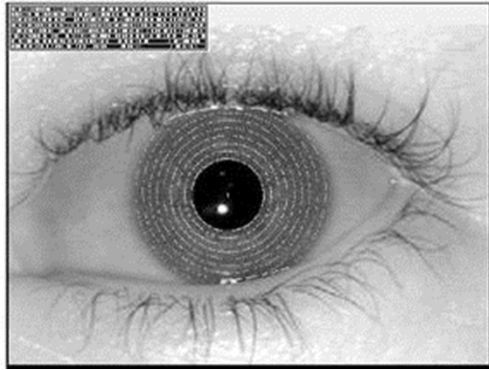
New

- Multiple Dictionaries
- Voice Recognition
- Diagram / Trigram / Phonemes

**Not Identification,
Is Command and Control**



Biometrics: Iris



Old

- Expensive camera
- Accurate in Ideal Situations



New

- Any camera, phone, or device with sufficient resolution
- Just software

Picture © Iridian Technologies, Inc.



Biometrics: Iris

- Deployments
 - Country Level
- Outstanding Issues
 - False positives: none yet
 - False negatives:
 - Patterned and light contacts



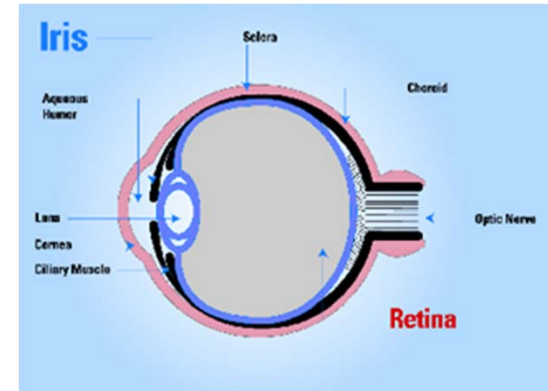
Biometrics:

- Non Starters

- Retina - too expensive
- Hand Geometry –not seen in a few years.

- Exotics

- DNA, Brain Waves - NWA (Neural Wave Analysis Interface), Skin Luminescence, Smell :->
- Never Started to take off



Yesterday

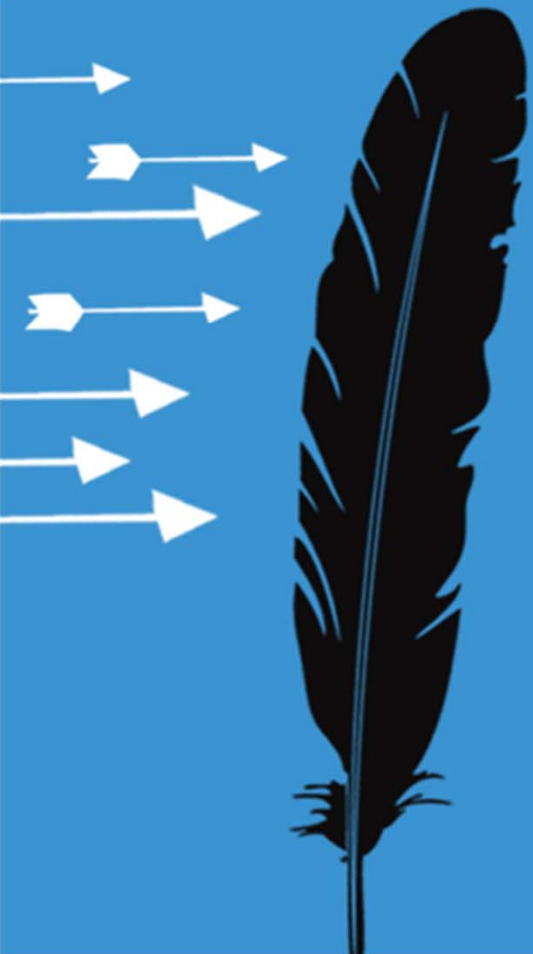
- Biometric technology was global
 - NIST Standard Program Interface - BIOAPI
- What controls the acquisition, propagation and dissemination of the biometric data raw or extrapolated (minutiae)?
- As usual, controls should have been put in place a decade ago – before standards.



Today

- Standards for
 - Programming Interfaces
 - Compliance Testing
 - Database interchange formats
 - Functional Testing
- Laws
 - Usage and controls (Illinois, Texas, etc)
 - Privacy concerns still abound
 - Covering data and use of data – what happens when the company goes out of business?
 - Beneficiaries - GLBA, SOX, HIPAA





Tokens

Authentication Tokens



Token Requirements

- Security Certification / Validation
 - FIPS 140-2 (Level 3 minimum)
 - Common Criteria (EAL 4 minimum)
- Types:
 - Stored Value
 - Asymmetric (PKI)
 - Symmetric Key (event- or time-based e.g. SecureID)
 - Contact & Contactless



Must Have High Attack Cost

- Cost: > \$100 per device
- Involve lots of people
- Slow: > 7 days
- Require a PhD or better ☺
- However...
 - Governments have infinite resources
 - Social engineering trumps all



Smart Cards — Obvious Attacks

- Re-Badging - My Face on your smart card
 - Acetone and a printer
 - Printers aren't that expensive
 - Chip replacement
 - Can be done by warming the card up, but can break the contacts
 - Delaminate
 - Split the card, and replace half
 - Older cards are easy to delaminate



Perception is Not Reality

- Lots of hacks
 - Cheap high-tech equipment
 - Logic Analyzers,
 - Disassemblers, specialized hardware
 - Massively parallel attacks
 - Infrastructure and social engineering attacks are easier
 - Spear-phishing Sykipot Trojan

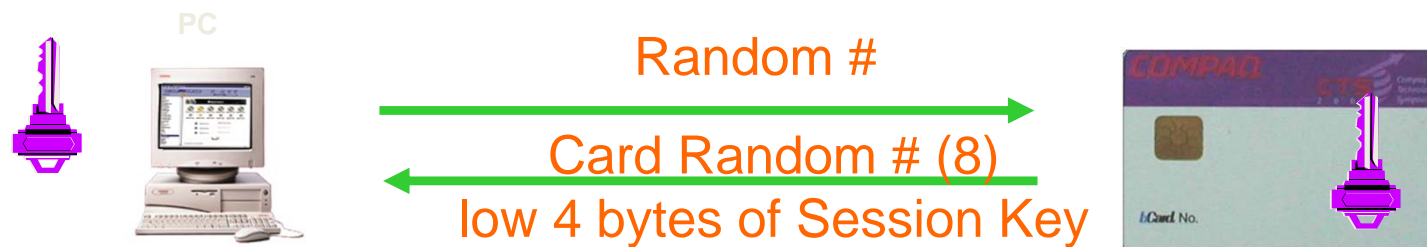


Smart Cards — Kick it Up a Notch

- Capture the communication path
 - Intercept the transaction:
 - Hardware
 - Buy a MAX-King card (not available in the US)
 - Buy a Breakout II device
 - Do it in software
 - Pure memory cards
 - susceptible to replay attacks



Smart Cards — Capture Attack

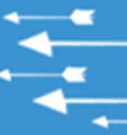


■ Capture Attack1

1. Capture security initiation and next transaction.
2. Send card random #s, until session key duplicates.
3. Replay last transaction

■ Capture Attack+

1. Commands are HMAC'ed with the session key
2. Guess session key high 4 bytes (2^{64} becomes 2^{32})
3. Validate the guessed key via HMAC
4. Send card random #s, until session key duplicates
5. Do your own transaction



Smart Cards — Kick it Up another Notch

- So if the random numbers ever duplicate you can:
 - Replay the transaction (boring)
 - Create your own transaction (more fun ☺)
- One note:
 - Older cards duplicate random numbers between .05 and 4% depending on the cards
- But Why Wait?
 - PIN Attack — Sykipot



Tokens: Contactless Smartcard Issue



- Unauthorized reading
 - distance is limited to ~ 4 inches.
 - ...or more with a non-standard antenna
- MiFare Classic Hacked
- MiFare DESfire Hacked

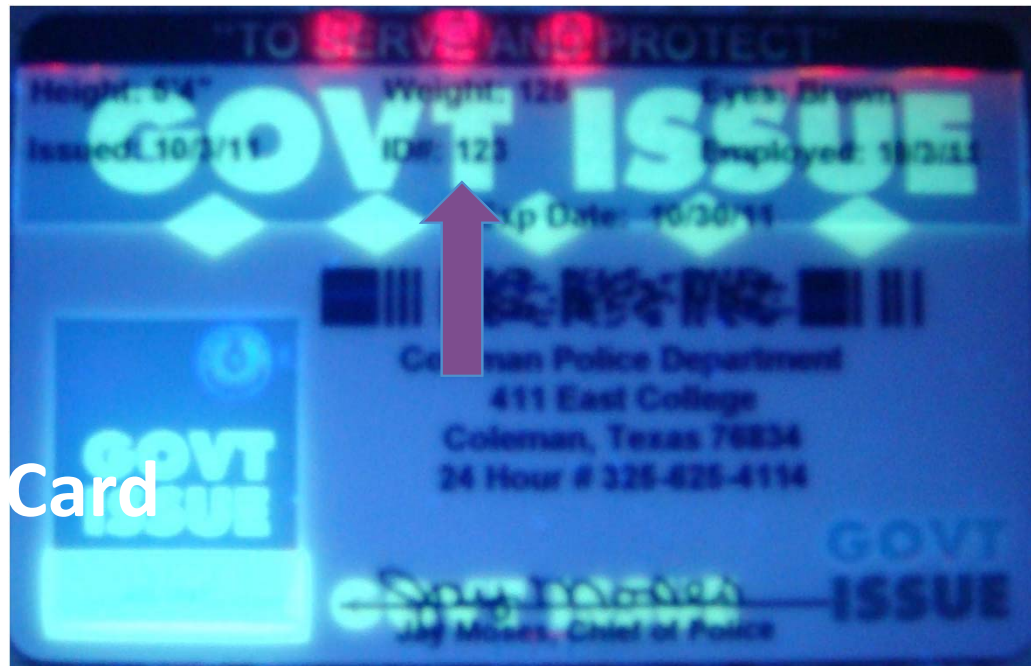


Action Items

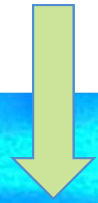
- How to protect yourself from authentication attacks
- Mitigate technical attacks against authentication
- Defense in depth
 - Multi-factor authentication
 - Separation of duties & networks
 - Encryption
 - Active auditing
- Train your employees to recognize and ignore social engineering attacks



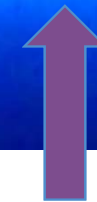
Smart Cards — Mitigating Physical Attacks



Smart Cards — Mitigating Physical Attacks



Front of Card



Back of Card



UV Light Source



Smart Cards — Mitigating PIN Attacks

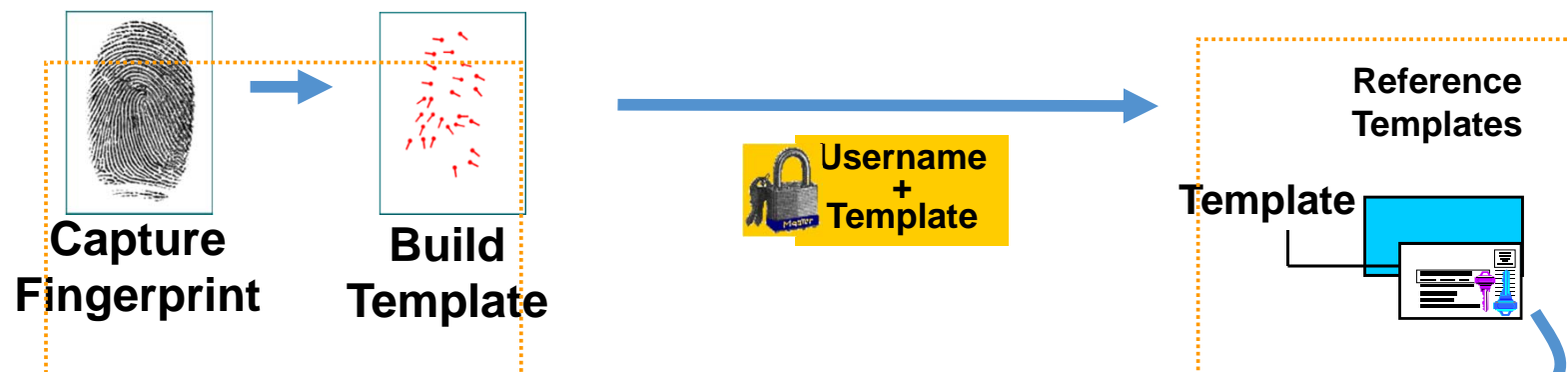


Smart Cards — Mitigating Comms Attacks

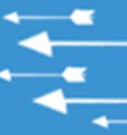
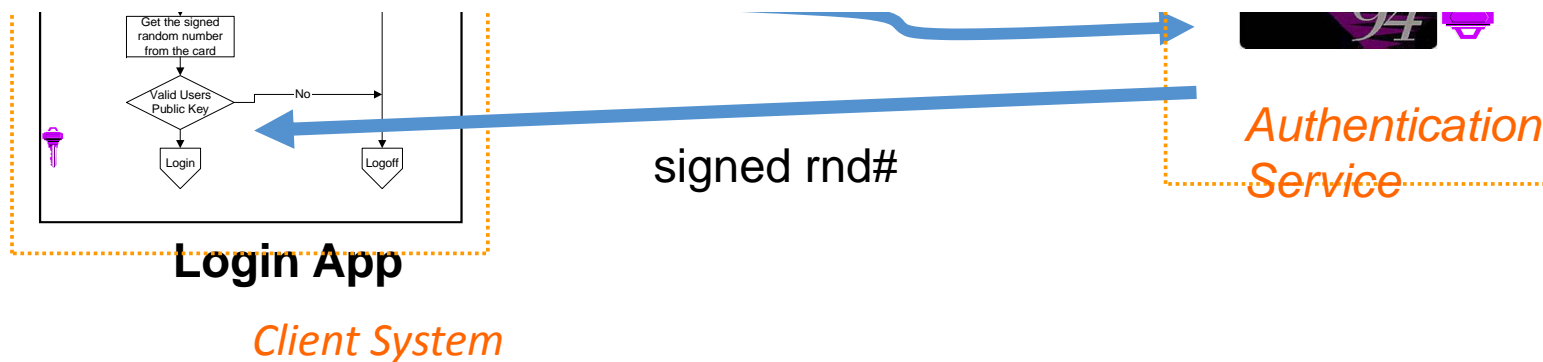
- Fix the Random # generators
 - No duplicate random # = no replay and
 - NO Guessing KeyS
- Protect communications between backend and card
 - Prevents PIN capture and MiM



Defense in Depth: 3 Factor



Not Really Changed!!!



More Defense in Depth

- Separation of duties and networks
 - <http://seacliffpartners.com/wordpress/?p=572>
 - <http://seacliffpartners.com/wordpress/?p=600>
- Full Disk Encryption may not be the answer
 - http://seacliffpartners.com/portfolio/CI_201110_Data_Loss_LaPedis.pdf
- Active Auditing
- Log engine with rules and real-time notification



Myths and Magic

Any sufficiently advanced technology is indistinguishable from magic

Arthur C. Clarke

- Myth
 - Biometric as encryption key
- Biometric authentication = fuzzy logic
 - Biometric read != exact same minutiae (replay attack)
- So
 - Biometric credentials cannot be used to generate absolute values (i.e. encryption keys)



Myth Busted (Almost)- Biometric On Board



- More Memory / Faster CPU on card
- Match on card
 - Unlocks signing capability
 - Unlocks encryption capability
- Messages to / from card can be signed / encrypted



Today — What is Next?

- National ID systems
 - Fingerprints
 - Face / IRIS recognition
- Public Safety
 - Face Location
 - Iris Recognition
 - No Registration Required
 - Social Media Mining
- Passports
 - RFID or Contactless
 - Or why bother when you can tell via face?



Conclusion

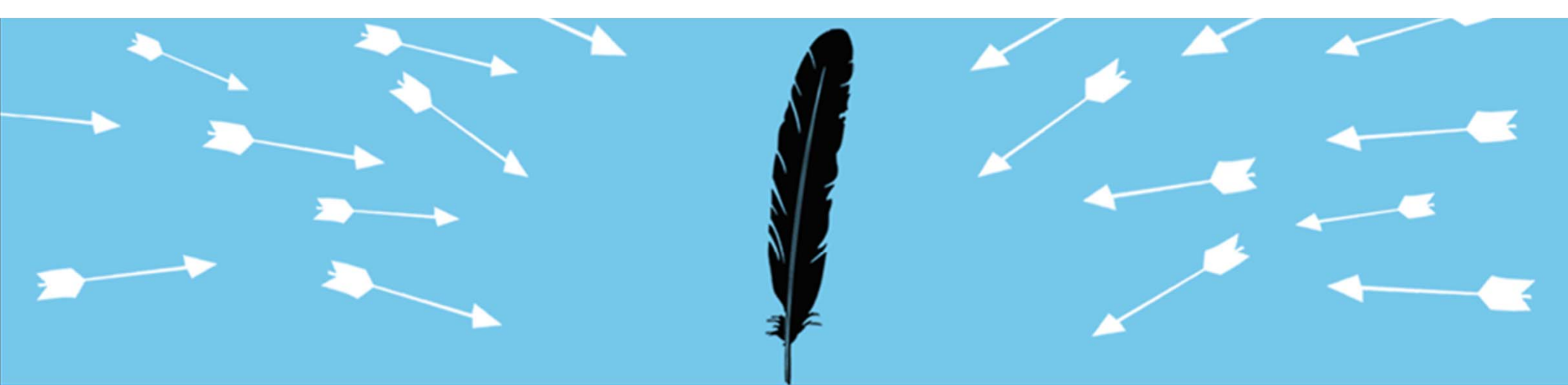
- Remember:
 - No perfect technology, enough persistence / money...
 - ANYthing can be hacked.
- Biometrics are OK as password replacements, but are better for ID and ease of use
- Biometrics & Token combinations provide better authentication than individual components.



Actionable Actions

- Other elements to reduce attack window i.e. Location + Time + ?
- Defense in depth is the best answer
- Need to mitigate social engineering





Biometrics and Access Token Technology, 10 Years Later... Contact Information

Michael F. Angelo, CRISC, CISSP

NetIQ Corporation

angelom@netiq.com

@mfa007

http://community.netiq.com/blogs/security_webb/

Ron LaPedis, CISSP-ISSAP, ISSMP

Seacliff Partners International, LLC

rlapedis@seacliffpartners.com

<http://seacliffpartners.com/wordpress/>

RSACONFERENCE2012



Backup?

Session ID:

Session Classification:

Defense in Depth - Two person control

- Person 1 provides PIN
- Person 2 provides biometric
 - What you have, what I know...





Rogues Technology Gallery

Session ID:

Session Classification:

Tokens: Buttons



Tokens: Shared Secret



Tokens: Challenge / Response



Tokens: USB Devices



Tokens: Smartcards

