BIO-CRYPTOGRAPHIC AUTHENTICATION

Terrance E. Boult

El Pomar Professor of Innovation and Security
University of Colorado at Colorado Springs
Also CEO/CTO Securics Inc

And R.C. Johnson PayPal
and Walter Scherirer Harvard Univ.

tboult@vast.uccs.edu 719 963 0573 (Cell)

UCCS Bachelor of Innovation™ University of Colorado Colorado Springs

Securics

HASHING/CRYPTOGRAPHY IS GREAT FOR PROTECTING PASSWORDS.

Hire Only SOUPS attendees
Hash is 417363bc444bf5fa42adb1d06eea011e

Fire Only SOUPS attendees
Hash is dd95e74883a289147db10d98f4cece4b

1 Bit change results in radically different Cryptostring

Since biometrics always change a little cannot just hash biometrics

Securics UCCS Bachelor of Innovation™

EXAMPLES OF PRIVACY ENHANCING TECHNOLOGIES FOR BIOMETRIC DATA

- Biometric Encryption (BE)
- Fuzzy Vaults (FV)
- Fuzzy Commitment (FC)
- Fuzzy Extractors (FE)
- Cancelable Templates (CT)
- Secure Sketch (SS)
- Biotopes and Vaulted Verification (VV)

Securics UCCS Bachelor of Innovation™

EXAMPLE: BIOMETRIC FUZZY VAULTS

- Alice places a secret κ in a fuzzy vault
  - κ is locked using a set of elements from some public universe U
  - κ is encoded in the coefficients of a d-degree polynomial p
  - Let V be points $((v_0, p(v_0)), \ldots, (v_n, p(v_n))$
  - Chaff point pairs (c_i, C_i) are randomly generated and inserted into V, then V is shuffled.
  - To unlock user must find at least d values v_i to recover p & κ.
- Each v_i must match exactly!

Securics UCCS Bachelor of Innovation™

CRACKING FUZZY VAULTS AND BE

- In our 2008 paper "Cracking Fuzzy Vaults and Biometric Encryption" we showed three new attacks that break FV and BE.
  - Attacks via Record Multiplicity (ARM)
  - Surreptitious Key-Inversion Attack (SKI)
  - Blended Substitution Attack
- For FV the problem stem from storing v_i & $p(v_i)$, e.g. ARM implies v_i reused so easily matched.
- Others have extended attacks to FC, FE, SS.
- Also, note that false accept rate (FAR) limits security/privacy – need high accuracy too.

Securics UCCS Bachelor of Innovation™

THE BIOTOPE INSIGHT….

→Break data into two parts, Stable and unstable!

- Stable part is transformed & encrypted/hashed to provide security/privacy and revocability
- Two parts together provide robust distance measure which we can prove will not decrease accuracy!

175 (stable) +1 unstable

165 (stable) – 4 unstable

- Can use stable data to embed keys.

Securics UCCS Bachelor of Innovation™

BIPARTATE BIOTOPE (W. SCHEIRER AND T. BOULT, "BIPARTITE BIOTOKENS: DEFINITION, IMPLEMENTATION, AND ANALYSIS," ICB 2009.)

	112 Bits GAR	112 Bits FAR	128 Bits GAR	128 Bits FAR	160 Bits GAR	160 Bits FAR
F.P. Fuzzy Vaults[1]	89	0.13	89	0.01	84	0
Password Vault[2]	88	?	86	?	79	?
Bipartite Biotokens	97	0	97	0	97	0

Comparison with Fuzzy Vaults on standard[illegible] known)

	192 Bits G[illegible]	256 Bits GAR	512 Bits GAR
FVC02 DB1	[illegible]7	94	95
FVC02 DB2	[illegible]7	97	92

Larger Key Sizes: tests wit[illegible] FAR in >1Billion trials

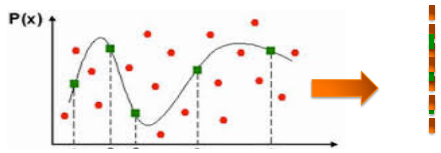
1. K. Nandakumar, A. K. Jain and S. Pankanti, "Fingerprint-based Fuzzy Vault: Implementation and Performance", In IEEE TIFS, vol. 2, no. 4, 2007

[illegible]. Nandakumar, A. Nagar and A. K. [illegible]ing Fingerprint Fuzzy Vault[illegible] Pas[illegible] Proc. of ICB 2[illegible]

BIPARTITE BIOTOPES AS A "FIXED FUZZY VAULT"

Recall problem stemmed from storing v_i & $p(v_i)$,

Bipartie NEVER ever stores v_i the value is secure and known attacks fail. However, user can generate v_i from raw biometric then while matching we associate with $p(v_i);P)$ and hence decode the bipartite vault.

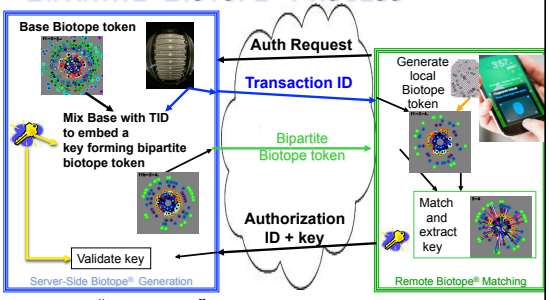


Revocable + nesting + embedding = Asymmetric ID

Securics

UCCS Bachelor of Innovation™ University of Colorado Colorado Springs

BIPARTITE BIOTOPE® PROCESS

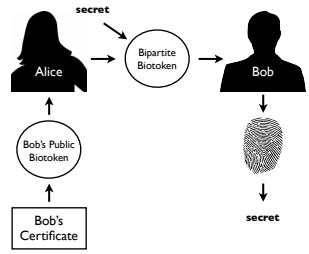


- Solves "asymmetry" of matching, Man in the Middle, Phishing and remote device hacks on "match" yes/no.
- Can be use "offline" with sync or to store encryption keys.
- Can be stored in X509-Certificate!

Securics

UCCS Bachelor of Innovation™ University of Colorado Colorado Springs

BIOCRYPTOGRAPHIC KEY INFRASTRUCTURE (BKI) USING BIPARTITE BIOTOKENS



Also Ideal for integration with PKI and federated identity solutions.

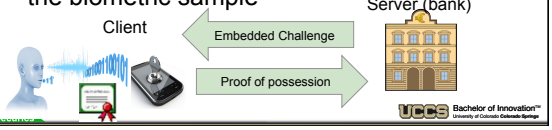
* W. Scheirer, W. Bishop and T. Boult "Beyond PKI: The Biocyptographic Key Infrastructure," IEEE WIFS 2010 Wksp on Information Forensics and Security

Securics

UCCS Bachelor of Innovation™ University of Colorado Colorado Springs

BKI VIA VAULTED VERIFICATION

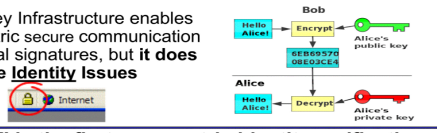
- Can we have BKI/Biometric verification without ever sharing biometrics?
- YES! VV is a challenge-response authentication. Can still do key release, but usually smaller keys.
- The biometric data is NEVER send off client device, but client can/must prove that it has the biometric sample



UCCS Bachelor of Innovation™ University of Colorado Colorado Springs

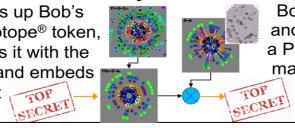
BASIC BKI SUMMARY

Public Key Infrastructure enables asymmetric secure communication and digital signatures, but **it does not solve Identity Issues**



Our BKI is the first asymmetric identity verification

Alice looks up Bob's Public Biotope® token, transforms it with the Trans-Id and embeds the secret



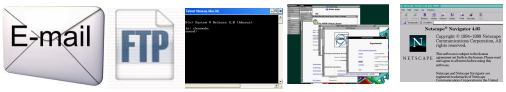
Bob's Fingerprint and keys generate a Private token and matching releases the secret

The revocable BKI technology is to biometrics what PKI/RSA was to encryption – a disruptive innovation based on asymmetric protection of information

Securics

UCCS Bachelor of Innovation™ University of Colorado Colorado Springs

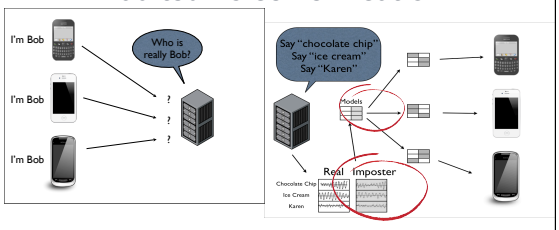
Remember the 80s and 90s?



- Huge explosion in new Internet protocols
  - Email, Remote Connections, The Web,…
- Security of these protocols was an afterthought!
  - We need cryptography to protect insecure channels
  - How can Alice verify a server?
  - How do we share encryption keys?

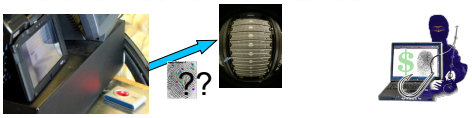
Solution: Public Key Infrastructure

Vaulted Voice Verification



- Johnson, R. C., and Terrance E. Boult. "With vaulted voice verification my voice is my key." Technologies for Homeland Security (HST), 2013 IEEE International Conference on. IEEE, 2013.
- Wilber, Michael J., Walter J. Scheirer, and Terrance E. Boult. "PRIVV: Private remote iris-authentication with Vaulted Verification." Computer Vision and Pattern Recognition Workshops (CVPRW), 2012 IEEE Computer Society Conference on. IEEE, 2012.
- Johnson, R. C., Walter J. Scheirer, and Terrance E. Boult. "Secure voice-based authentication for mobile devices: vaulted voice verification." SPIE Defense, Security, and Sensing. International Society for Optics and Photonics, 2013.
- Johnson, R., Boult, T. E., and Scheirer, W. J. (2013a). Voice authentication using short phrases: Examining accuracy, security and privacy issues. Biometrics: Theory, Applications and Systems (BTAS) 2013

Biometrics for Verified Identity?

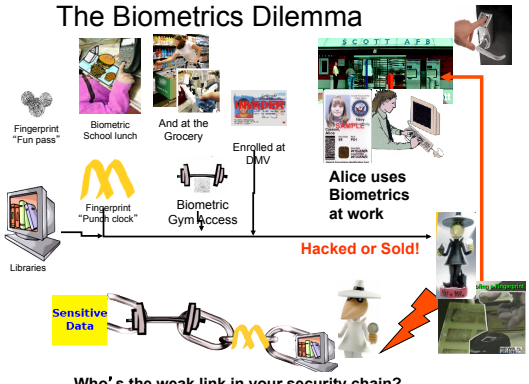


Biometrics provide identity assurance, convenient & low cost but

- Cannot revoke a fingerprint like a password or credit card!
- Like symmetric encryption both sides need the "secret"
- Only matching party can really trust match happened, other party must trust the matcher with their data!
- Doppleganger Attacks not impacted by "liveness" so data must be protected.

How can we address privacy/security concerns to achieve truly usable biometrics?

The Biometrics Dilemma

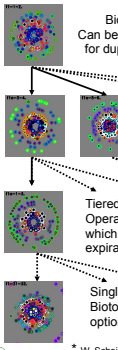


Who's the weak link in your security chain?

BKI Advantages

- Reduce user friction by addressing privacy concerns while improving security
- Cloud-stored strong identities
- Asymmetric identity modeling
- Move "identity" into the digital signature/ key management space
- New models for secure payment

BKI: Biocyptographic Key Infrastructure



Biotoken® rootID Can be used to search and for duplicate enrollments

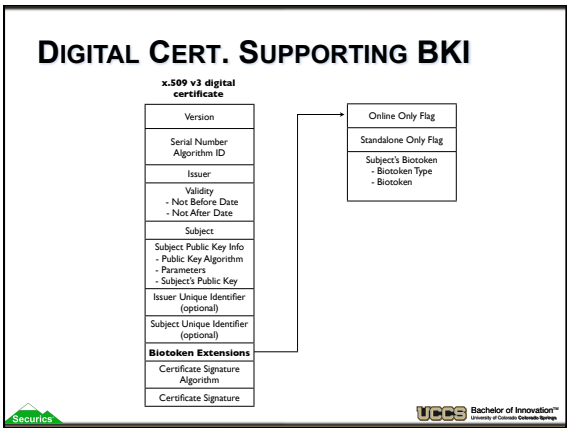
Root Signed Biotoken® Master IDs One per application

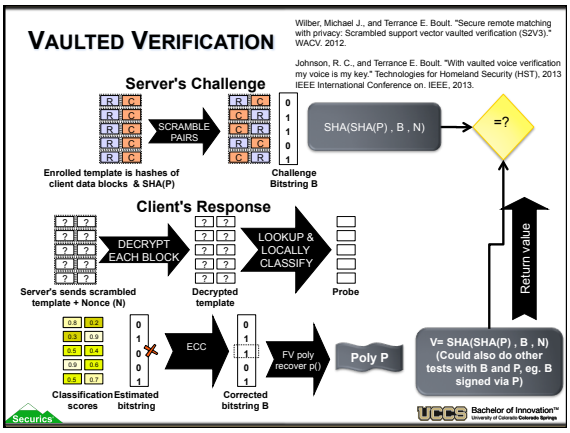
Tiered-BCA signed Operational Biotope® IDs which can have date-driven expiration.

Single use Bipartite Biotope® tokens with optional embedded data

- Add Biotope fields & dates in X509 v3 Cert extension fields.
- BCA proofs ID, issues and signs user's "root" certificate
- BCA derives operational certificate and return it or publishes in a private or public directory.
- Alice can locate Bob's cert, derives new transaction certificate with embed key. She signs cert and sends to Bob.
- Bob can validate the message, use biometrics to extract key use or sign it to validate transaction and identities.

* W. Scheirer, W. Bishop and T. Boult "Beyond PKI: The Biocyptographic Key Infrastructure," IEEE WIFS 2010 Wksp on Information Forensics and Security


DIGITAL CERT. SUPPORTING BKI
x.509 v3 digital certificate
Version
Serial Number Algorithm ID
Issuer
Validity - Not Before Date - Not After Date
Subject
Subject Public Key Info - Public Key Algorithm - Parameters - Subject's Public Key
Issuer Unique Identifier (optional)
Subject Unique Identifier (optional)
Biotoken Extensions
Certificate Signature Algorithm
Certificate Signature
Online Only Flag
Standalone Only Flag
Subject's Biotoken - Biotoken Type - Biotoken
Securics
UCCS Bachelor of Innovation


VAULTED VERIFICATION
Wilber, Michael J., and Terrance E. Boult. "Secure remote matching with privacy: Scrambled support vector vaulted verification (S2V3)." WACV. 2012.
Johnson, R. C., and Terrance E. Boult. "With vaulted voice verification my voice is my key." Technologies for Homeland Security (HST), 2013 IEEE International Conference on. IEEE, 2013.
Server's Challenge
SCRAMBLE PAIRS
Enrolled template is hashes of client data blocks & SHA(P)
Challenge Bitstring B
SHA(SHA(P) , B , N)
=?
Client's Response
DECRYPT EACH BLOCK
LOOKUP & LOCALLY CLASSIFY
Server's sends scrambled template + Nonce (N)
Decrypted template
Probe
Return value
ECC
FV poly recover p()
Poly P
V= SHA(SHA(P) , B , N) (Could also do other tests with B and P, eg. B signed via P)
Classification scores
Estimated bitstring
Corrected bitstring B
Securics
UCCS Bachelor of Innovation