Attacking Biometric Access Control Systems

By: Zamboni

Outline

- Overview of biometrics
- General methodology used to attack biometric systems
- Example attacks against physical access control systems
- Defenses
- Question

Biometrics

- Unique and (relatively) permanent physical or behavioral characteristic that can be used to identify or authenticate a user
- Examples:
  - Finger prints
  - Hand geometry
  - Vascular patterns
  - Retina
  - Iris
  - Voice pattern
- Advantages
  - Unique
  - Part of the user
  - Very hard to forgot or lose
  - Can provide reliable authentication

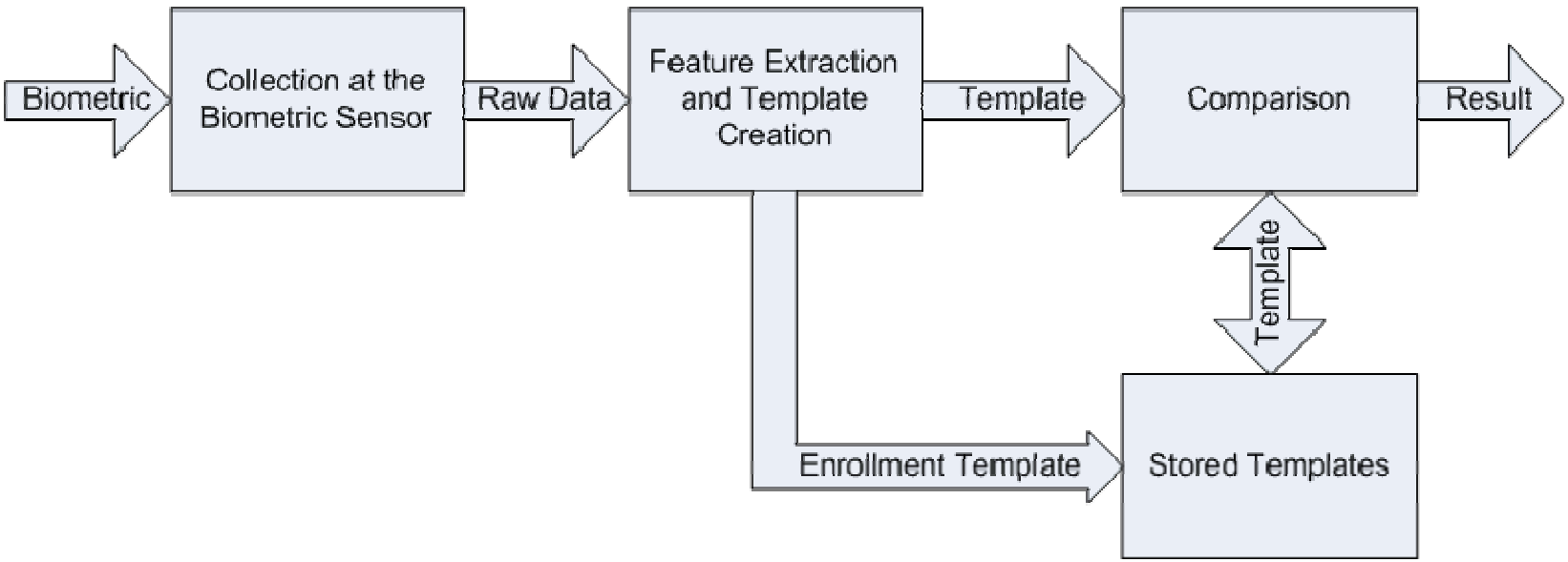
Disadvantages & Problems

- Cannot be kept secret
- Some can be copied or stolen
- Cannot be reset or revoked
- Make insecure cryptographic keys
- Common across multiple systems/organizations
- System accuracy is dependent on enrollment verification
- System can be manipulated if more than one person has access to the reader or resource

Basic Biometric Process

1. Collection at the Biometric Sensor: System captures physical or behavioral characteristic
2. Feature Extraction: Template is created
3. Comparison: New template is compared with stored templates to produce a matching score
4. Result: System returns a match or non-match result

Basic Biometric Process



Identification vs. Authentication

- Identification tells who someone is
- Authentication verifies that someone is who he/she claims to be
- Types of authentication:
  - Something you know
  - Something you have
  - Something you are

Template Verification

- Identification
  - *One-to-many search*
  - Does the system recognize you?
  - Steps:
    - 1) User presents a characteristic to the system
    - 2) User template is compared to each template in the database for a match
- Authentication (Verification or positive matching)
  - *One-to-one search*
  - Are you who you claim to be?
  - Steps:
    - 1) User provides user name, PIN or other form of identification
    - 2) User presents a characteristic to the system
    - 3) User template is only compared to template associated with that specific user

Template Matching

- Matching is approximate
- Problems with this
  - Can not give a categorical yes or no
  - Can only say that templates match with a confidence level of 99%
- AKA: Loose equality or close equality

Error Rates

- Type I – FRR (False Reject Rate)
  - Rate at which system denies access to a legitimate user
- Type II – FAR (False Acceptance Rate)
  - Rate at which system authenticates an un-enrolled user
  - Important: Even without an intruder a system could wrongly authenticate a user
- CER: Cross-over Error Rate (Equal Error Rate)
  - Point at which Type I and Type II errors are equal
  - Most realistic and reasonable rate to use when comparing biometric systems

Attacking Biometric Systems

General Attack Information

- Security is only as good as the weakest link
- Try traditional attacks first
  - Traffic replay
  - Spoofing
  - Password guessing
  - Bruteforce
- Examine system connections
  - How secure are the connections?
- Proprietary systems: security through obscurity
  - Download vendor's docs and look for default passwords, SNMP strings, etc
  - Often vulnerable to traditional attacks
- Attack Windows and Unix systems which are part of the biometric system like you would any other Windows or Unix box
- Know the OEM
  - Find the OEM for the device; research known exploits against their products
  - Find other manufactures that source from that OEM and research exploits against their products

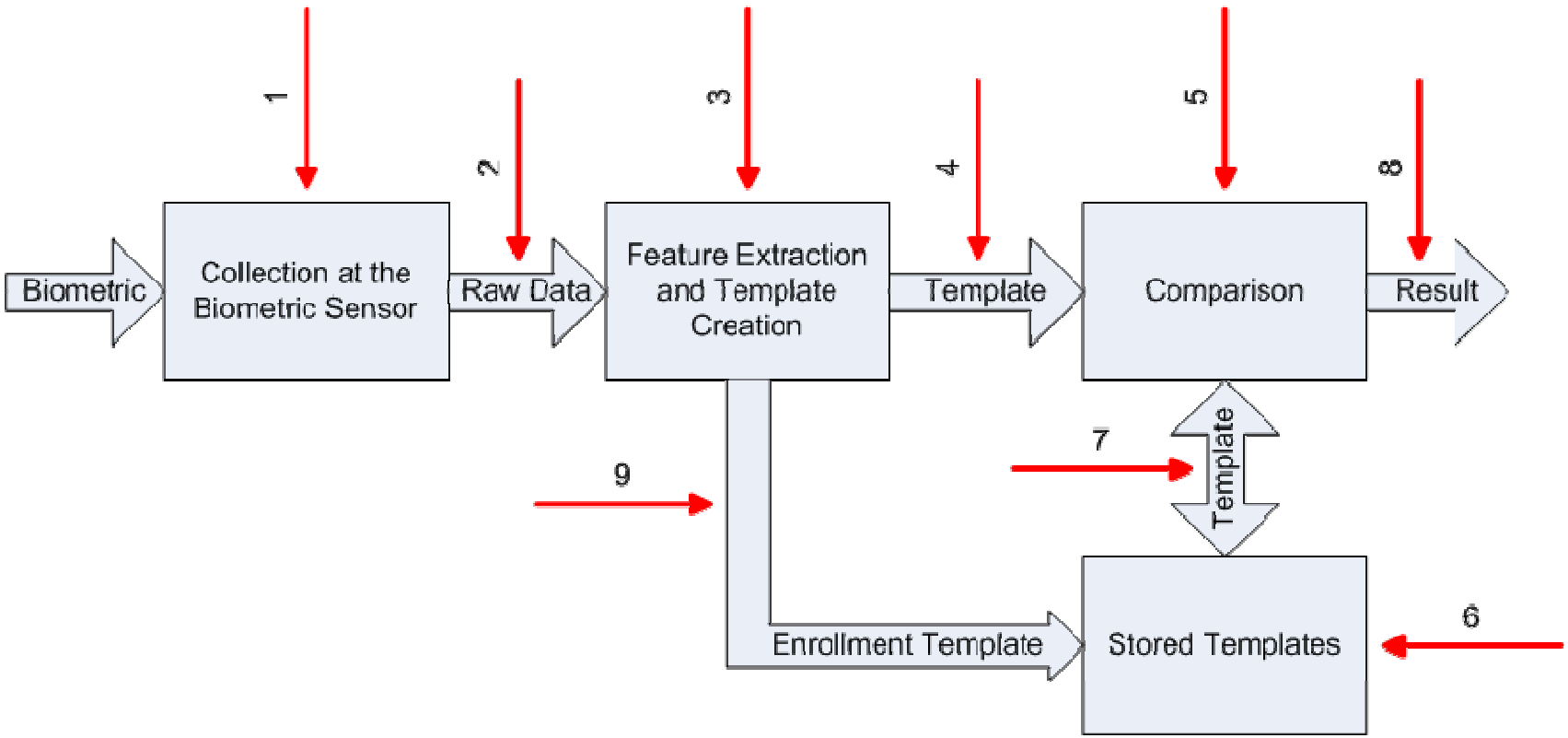
Words of Caution

- Some systems are fragile
  - Even a simple portscan can crash some systems
  - Approach readers and panels with caution
  - System instability could be caused by misconfiguration
    - Very common: misconfigured Lantronix Micro100 serial server
      - Recommend excluding port 30718 from port scans
  - Others are intrinsic product flaws
- If possible test attacks first in a lab or non-production environment

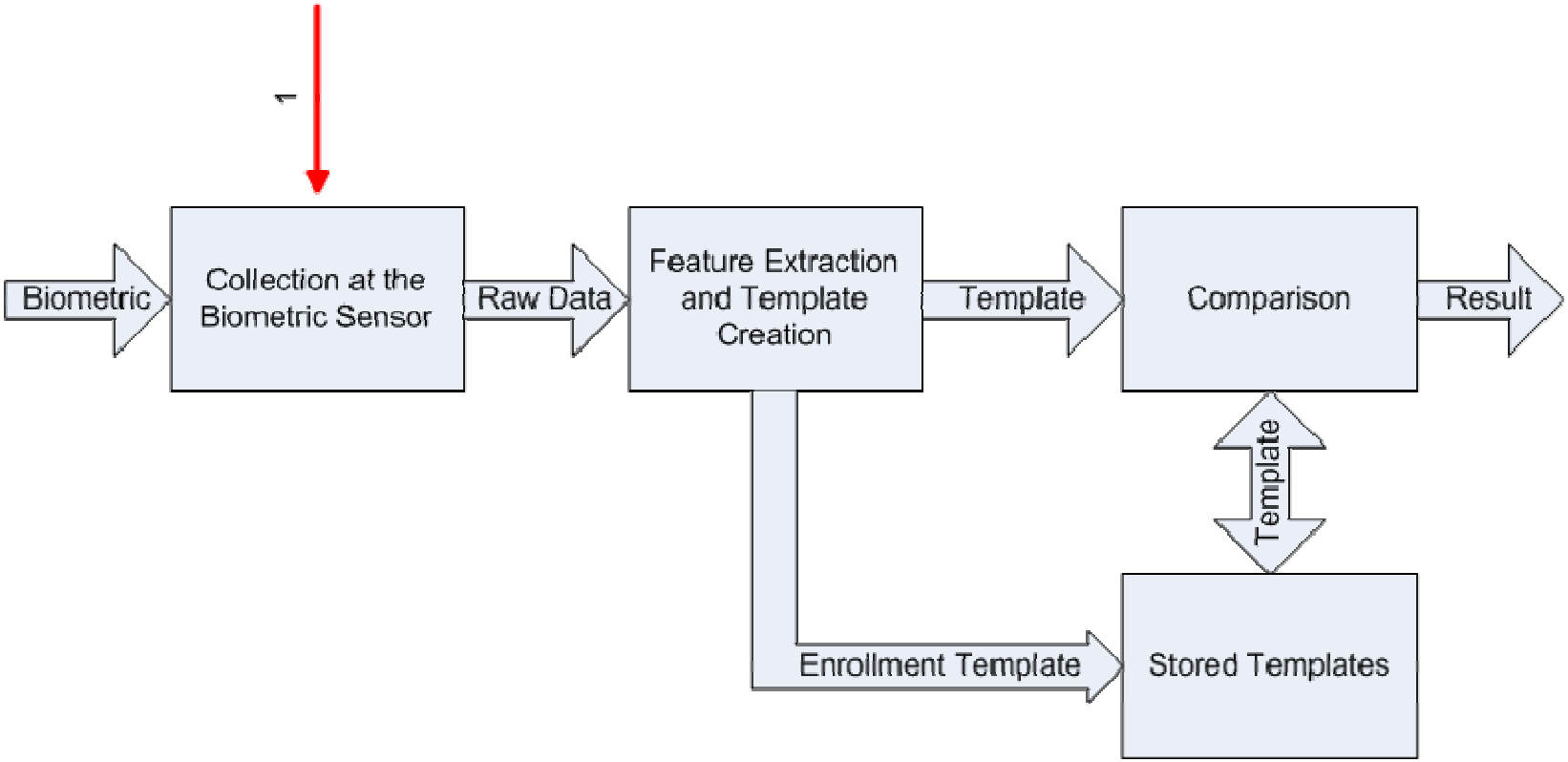
Nine Generic Attack Points

- Overview of where to attack a biometric system
- General methodology can be applied to all biometric systems
- N.M. Ratha, J.H. Connell and R.M. Bolle: “An Analysis of Minutiae Matching Strength”
  - 8 attack points
- Ninth point

Attack Points



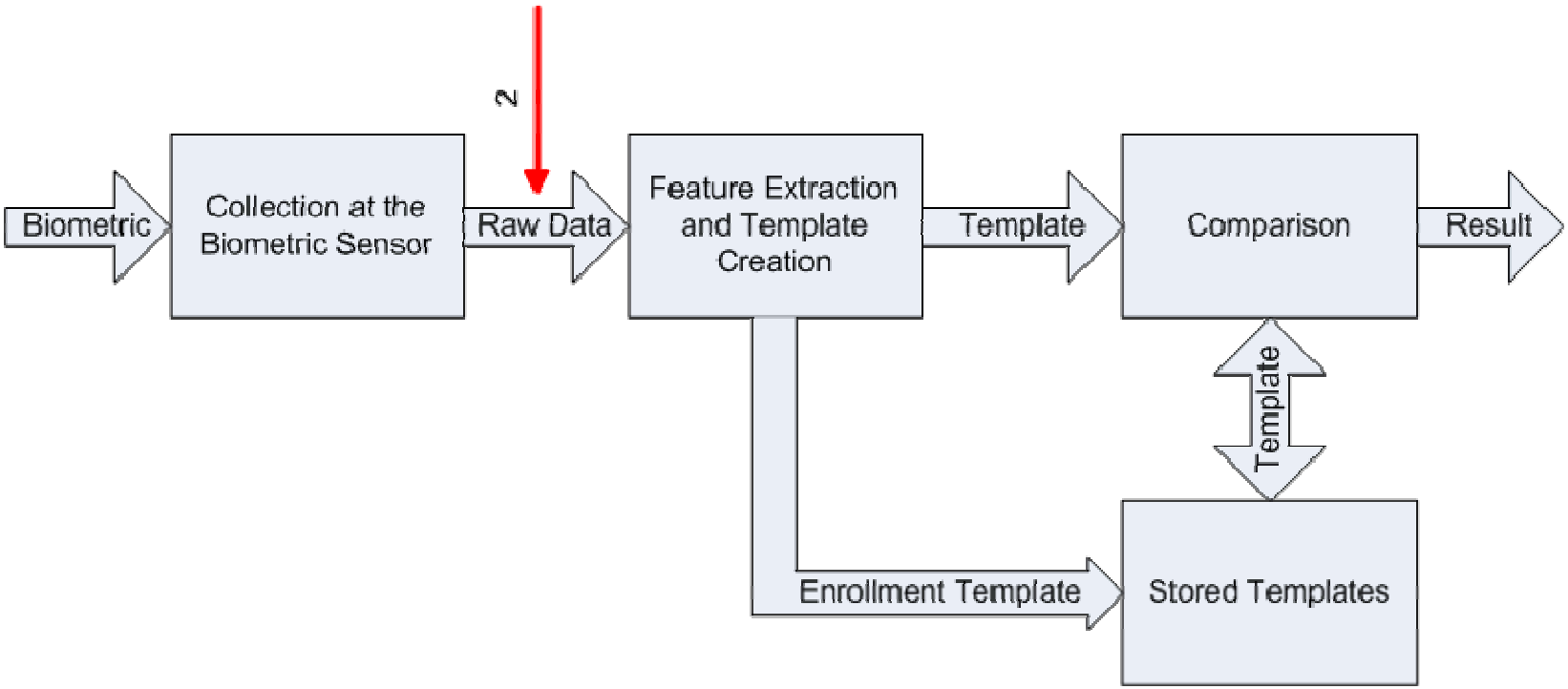
Type 1 Attack



Type 1 Attack

- Attacking the biometric sensor
- Present a fake biometric to the sensor that mimics an authorized user.
- Examples:
  - Fake gelatin fingers
  - Picture of an iris
  - Voice recording

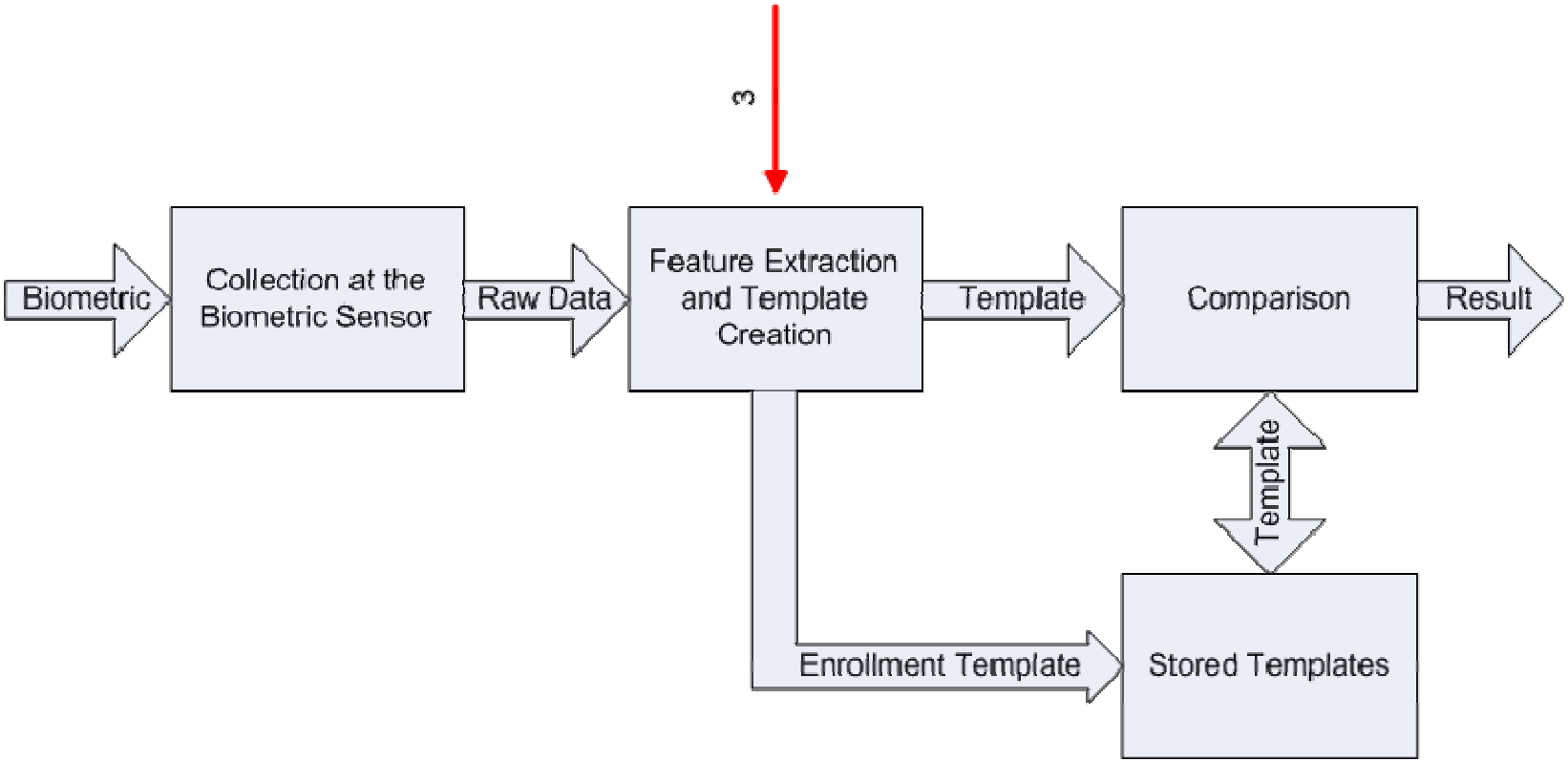
Type 2 Attack



Type 2 Attack

- Attacking communications from the biometric sensor
- Not always an option: biometric sensor and feature extractor are sometimes combined
- Attacker can intercept data sent by sensor
- Attacker could send malicious data to the feature extractor
  - Replay attack
- Examples:
  - Hill Climbing attack
  - Decoding intercepted WSQ files to make fake fingerprints
  - Injecting malicious WSQ files into the system

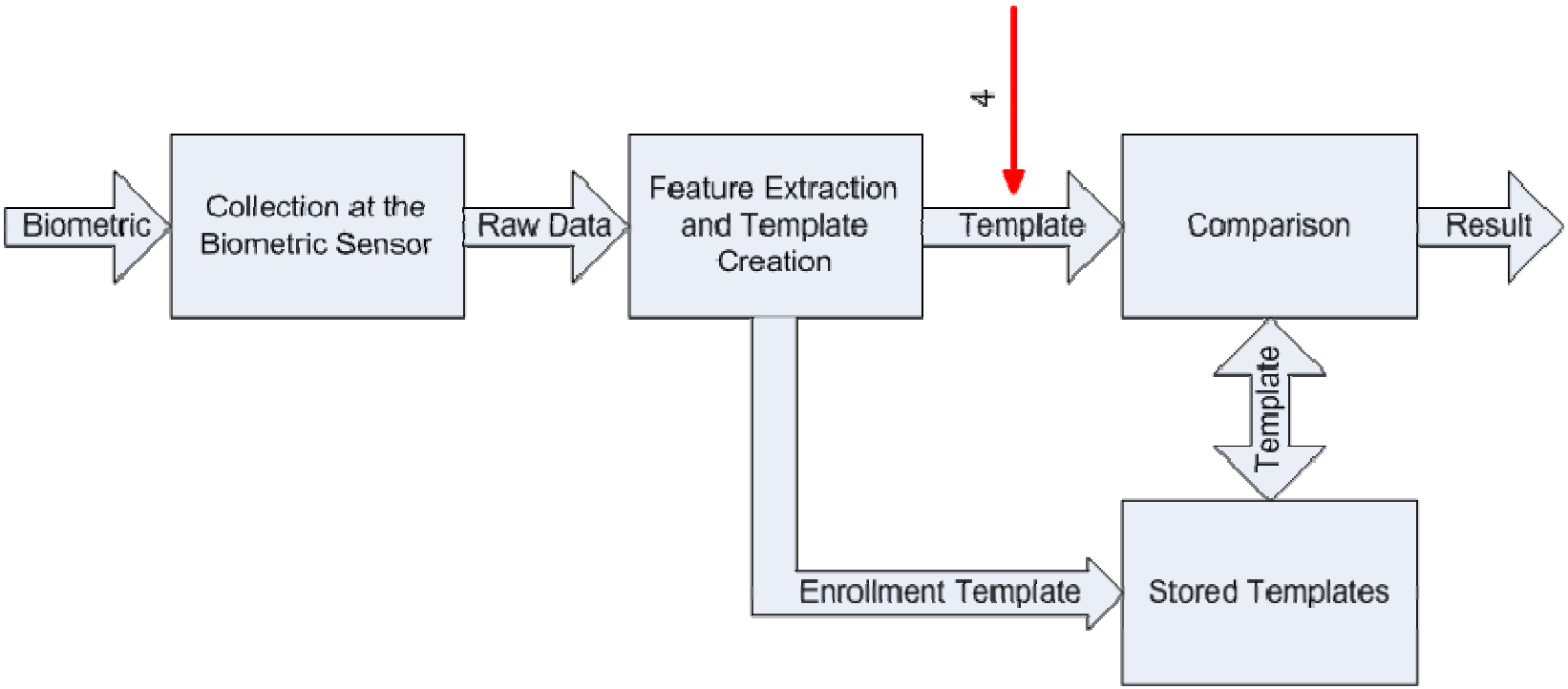
Type 3 Attack



Type 3 Attack

- Manipulating/overriding feature extraction and template creation process
- Usually an attack on software or firmware
- Examples:
  - Generating a template preselected by the attacker
  - Steal templates generated by the system

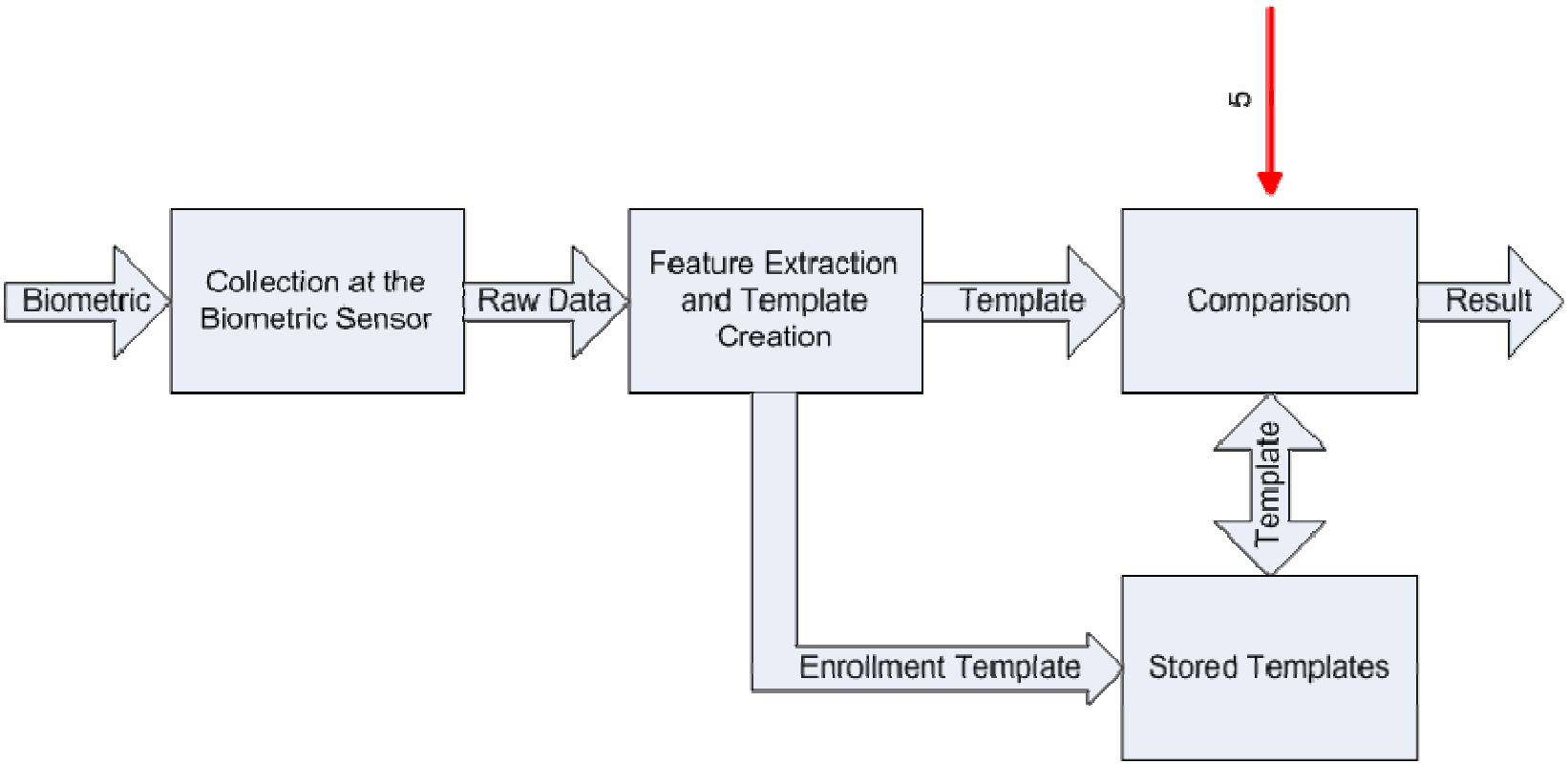
Type 4 Attack



Type 4 Attack

- Attacking the communication channel between template creation unit and the comparison unit
- Large threat when templates are compared on a remote system
- Examples:
  - Intercept a valid user template for later use
  - Inject a malicious template
  - Inject malicious templates to bruteforce the system
    - Easier to inject bruteforce traffic here than when it leaves the biometric sensor
    - Templates are simpler than unprocessed biometric
    - Smaller keyspace
    - Not a very useful attack without knowing template format

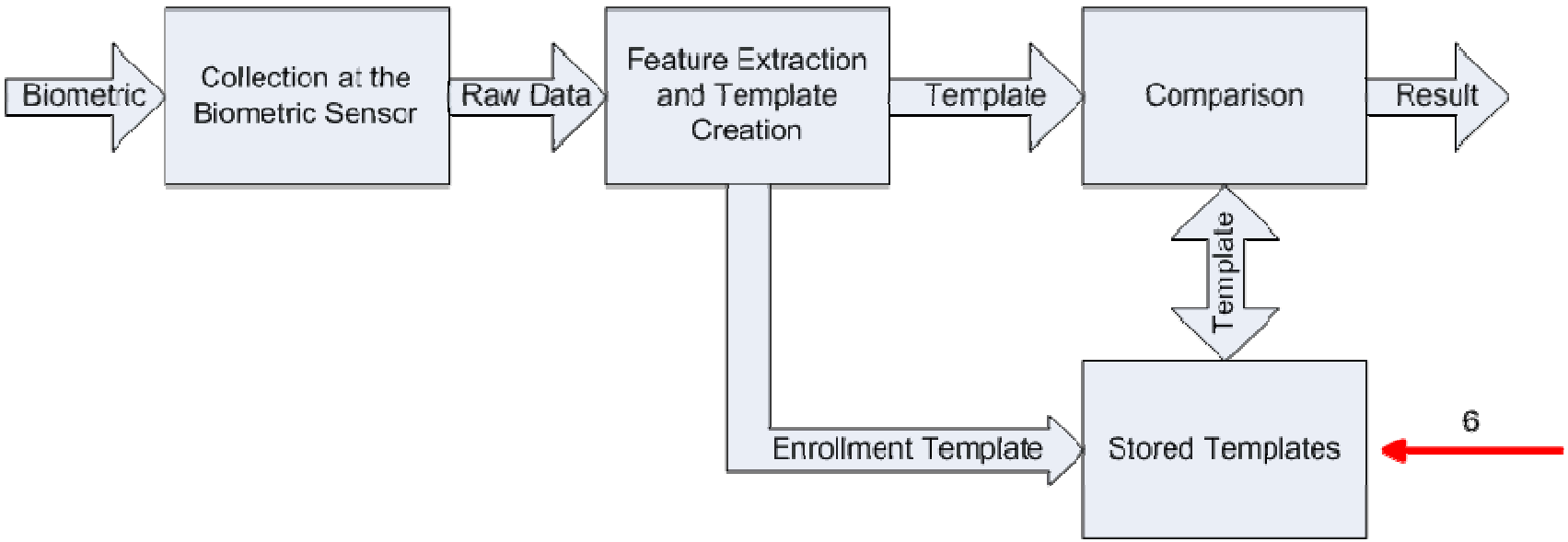
Type 5 Attack



Type 5 Attack

- Attacking the template comparison unit
- Close equality makes some attacks possible here
- Templates must be in the clear when they are compared
- Can be an attack on software, firmware or configuration
- Examples:
  - Modify matching software to produce artificially low or high scores
  - Change the threshold for a successful match
    - Can make spoofing attacks easier
    - End users will not notice this change because system will continue to authenticate them
    - Some systems have a lower limit on the matching score threshold
    - On some systems the setting is configurable over the network or configurable locally with the appropriate software package and a PDA.

Type 6 Attack



Type 6 Attack

- Attack or tamper with stored templates
- Some systems support more than one template per user
  - Beware of duress templates(!)
- Examples:
  - Steal a template
  - Associate a malicious template with an already enrolled user
  - Enroll a malicious user

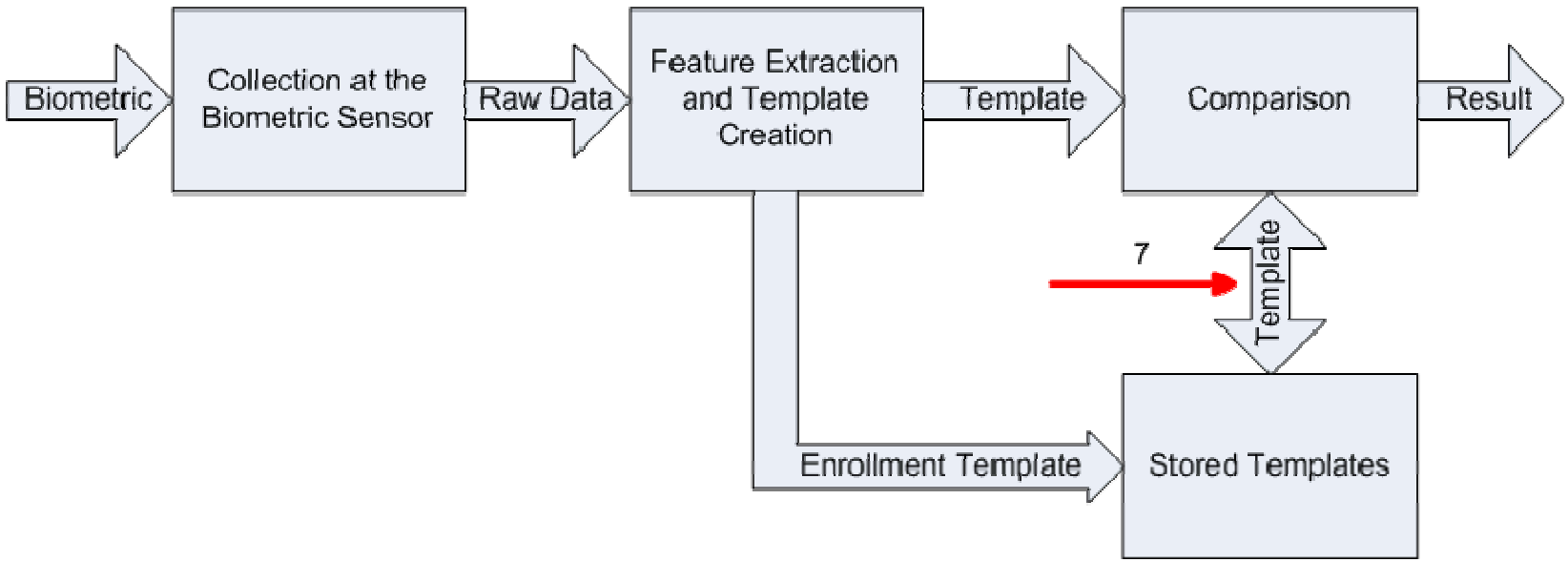
Four Ways to Store Templates

- On Reader or Device
  - Quick
  - No network access required
  - Limited storage space
  - Inconvenient manual loading
- Central Server
  - Efficient management of multiple users across multiple systems
  - Dependant on a network
  - Backend server can be attacked
  - Transportation and storage security a concern
- Access Card or Token
  - Quick
  - User controls the template
  - Token or access card can be stolen
  - Need to worry about secure storage and transmission
- Hybrid – Combination of the above
  - Examples:
    - Templates stored on a central server but cached on the reader
    - Templates stored on a smartcard and stored on central server to make rebadging easier

Type 6 (Cont.)

- Central server:
  - Template usually stored in a database or flat file
  - Try traditional attacks
- Access card or token
  - Attacks on proximity cards
  - Poor read/write protection RFID
- Acquiring a template to inject
  - Steal from a central server, card or reader
  - Buy a reader and create your own templates
    - Template created on company X, model Y systems will work on all model Y system by company X

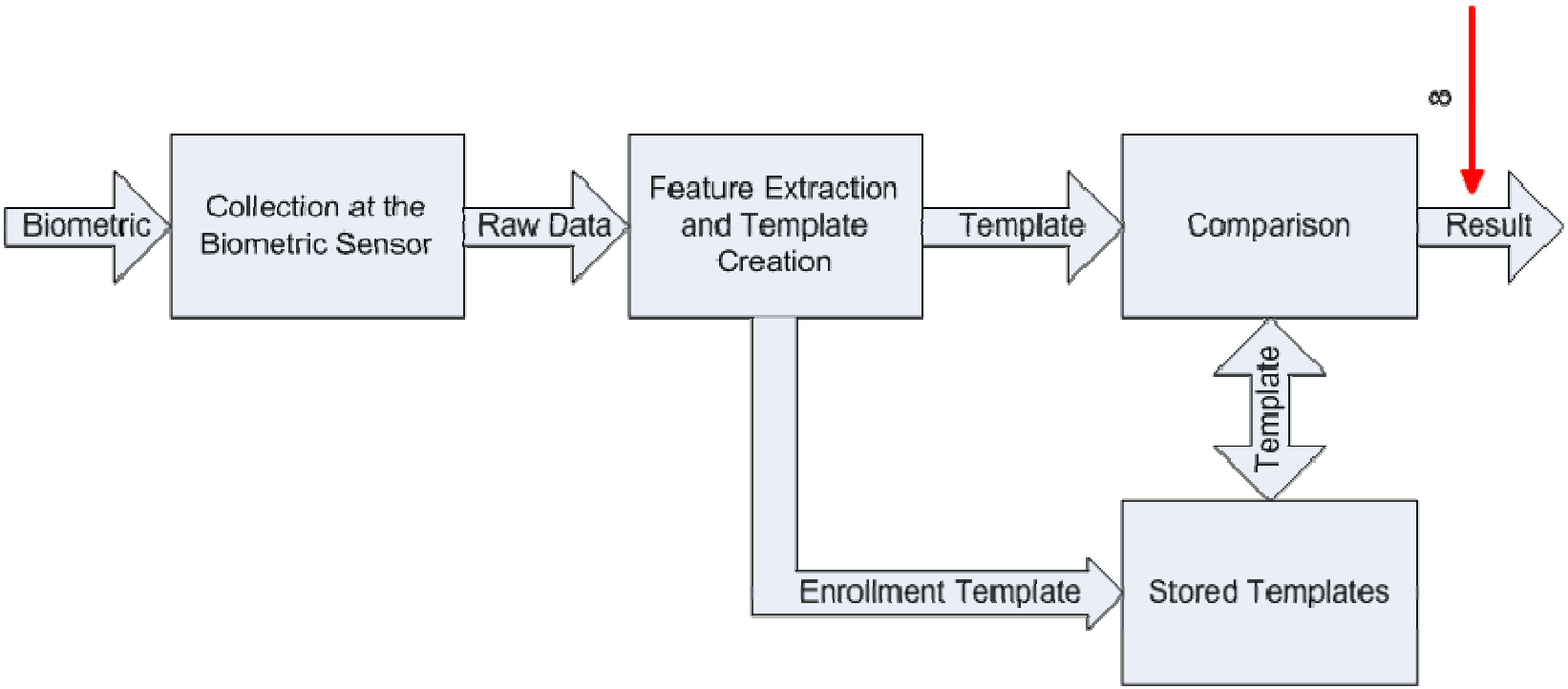
Type 7 Attack



Type 7 Attack

- Attacking the transmission of stored templates
- Data can be corrupted, intercepted or modified
- Traffic is often unencrypted when send over Ethernet or serial networks
- Templates stored on cards or tokens:
  - RFID usually transmits in the clear
    - Parts of Mifare and HID iClass transmissions are encrypted
  - Recent attack on the Texas Instruments DST chips
  - Replay attacks on proximity cards
- Examples:
  - Sniffing traffic to steal templates
  - Injecting templates to falsely authenticate a malicious user

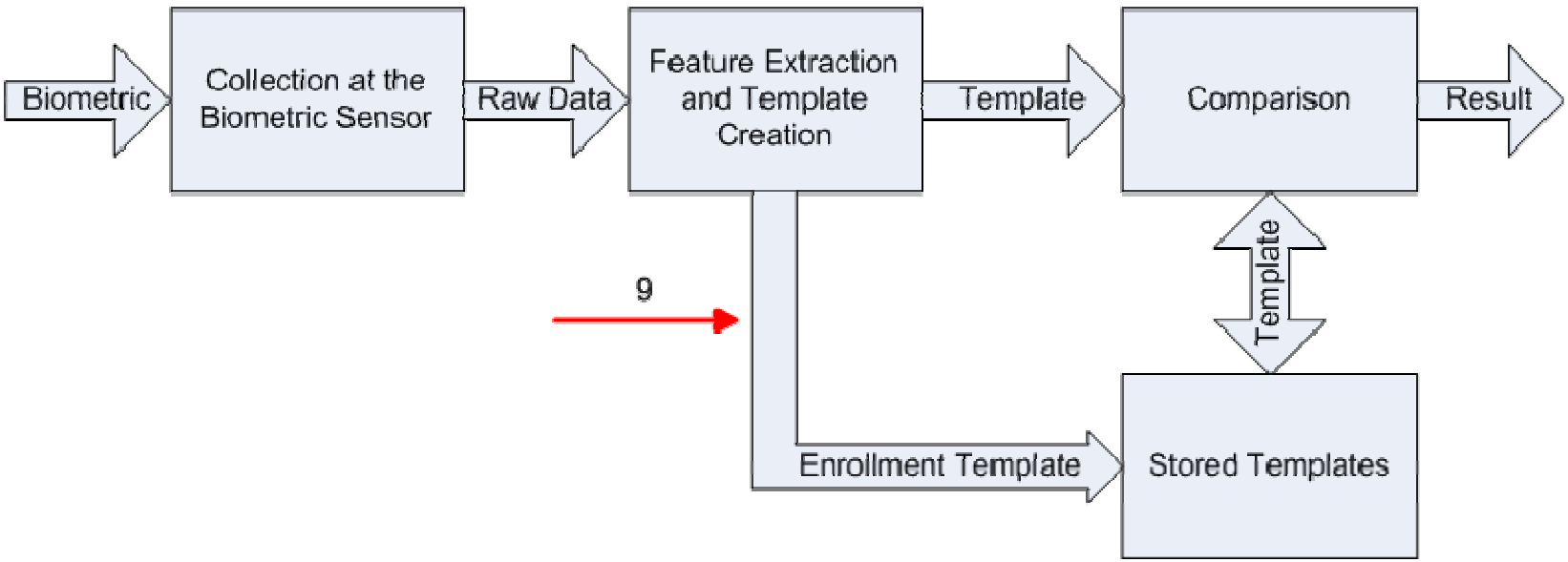
Type 8 Attack



Type 8 Attack

- Overriding the final decision
- If the final match decision can be overridden by an attacker than the system has been defeated

Type 9 Attack



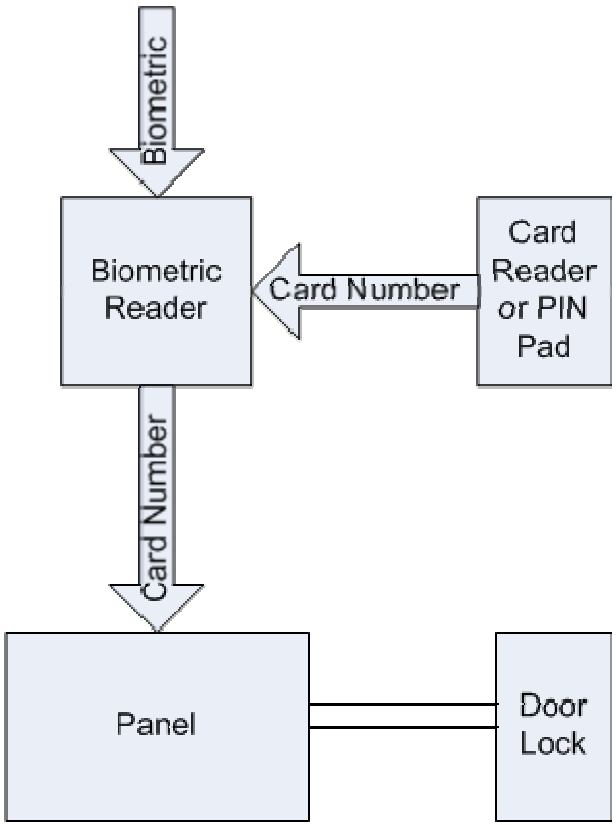
Type 9 Attack

- Attacking the transmission of enrollment templates to the storage location
- Similar to attacks at point 4 but with potential longer lasting affects
  - Could permanently add malicious template into the system

Examples

Names withheld to protect the triumphant

Simple Biometric Access Control System



- Common setup used by many biometric readers that store templates on the reader

- Step to authenticate a user:

1. User presents card or enters PIN
2. PIN or card number is sent to the biometric reader
3. Reader finds template for the user
4. Reader compares templates
5. If they match the PIN or card number are send to the access control panel
6. If that user has access to that door the control panel unlocks the door

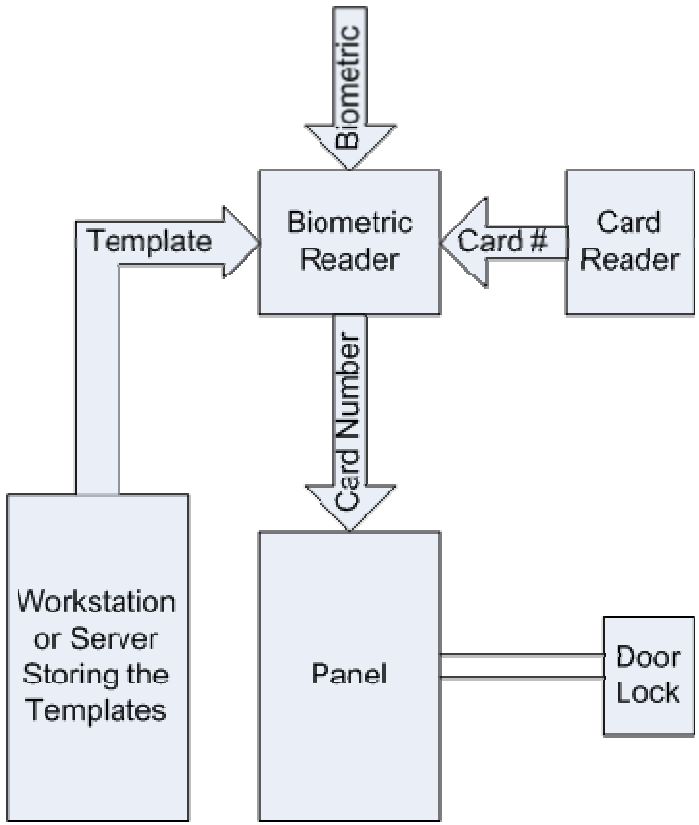
Using Wiegand Injection

- Inject the card number of a legitimate user into a Wiegand line
  - Using a Wiegand magcard reader
    1. Gain access to the Wiegand line for the Biometric reading
       - Remove Biometric reader from wall
       - Access wires in drop ceiling or other non-secure area
    2. Connect the Wiegand magcard reader to the Wiegand line
    3. Create a custom magcard with the card number of the user you wish to impersonate
    4. Swipe card through reader to send card number
    5. Open door
  - Using a RS-232 to Wiegand converter
    1. Gain access to the Wiegand line for the Biometric reading
       - Remove Biometric reader from wall
       - Access wires in drop ceiling or other non-secure area
    2. Connect the RS-232 to Wiegand converter
    3. Send card number
    4. Open door

Using Wiegand Injection Defenses

- Defense:
  - Install tamper switches on readers
  - Monitor for communication errors from readers
  - Change keycode on locks used to secure readers
  - If possible use high security locks to secure readers and panels
  - Protect all Wiegand lines using hard conduit
  - Have camera coverage on all readers

Biometric System with Templates at a Central Location



- Step to authenticate a user:

1. User presents card
2. Card number is sent to the biometric reader
3. Reader request template for that user
4. Server sends template to the reader
5. Reader compares templates
6. If templates match, the card number is send to access control panel
7. If that user has access to that door control panel unlocks the door

Attacking the Central Server

- MSDE used to store the templates
  - Unpatched by default
  - Weak SA password
- Steps to attack the templates on the server
  1. Gain access to the database using know vulnerability
  2. Locate the templates
  3. Associate an already enrolled user template with a user who has higher access privileges
- Defenses:
  - Patch and harden the system used to store the templates
  - Monitor for intrusions on the system
- Note: PIN or card number stored in the clear in the database
- Beware of injecting duress templates

Defenses: Things You Can Do

- Test systems to know their weakness so threats can be better mitigated
- Use man traps to allow only one person to have access to the biometric reader at once.
- Monitor for false readings/failed authentication attempts
- Have a camera covering each reader
- Harden and patch all servers and workstations in the biometric system
- Install tamper switches on all readers
- Activate liveliness detection on all readers
- Combine biometrics with a second or third form of authentication

Defenses: Vendor Action

- Add time stamp and sequence number to data in order to prevent reply attacks
- Output matching scores in wider increments to protect against Hill Climbing attacks
- Mutually authenticate readers and panels/backend servers
- Encrypt all data transmissions using proven encryption algorithms
- Install server and workstation software as secure by default

Conclusion

- Use the nine attack types to locate weak points in a system
- Try traditional attacks first
- Only way to determine how secure a biometric systems is to:
  - Test it yourself
  - Attack it yourself
  - Break it yourself
- Physical security people will need help to do this

Questions?

Zamboni@Miskatoniclabs.com

www.miskatoniclabs.com/biometrics/