

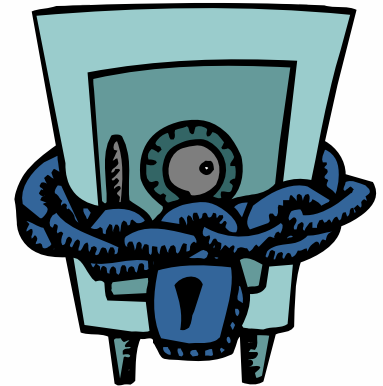


Biometric Security: Client-Server Systems

Mira LaCous
VP Technology & Development
BIO-key International, Inc.
651-789-6117
Mira.LaCous@bio-key.com

The Session

- Private vs Public / Personal vs Public
- Forms of Attack
- Forms of Failure
- Risks of Attack and Failure
- The Need for Security
- How to Implement Security
- Wrap up & Questions



The Need

- Protect systems, data and facilities by
 - Preventing false entry.
 - Tracking access.
 - Ultimately providing simpler access, with security.
- Protect privacy by
 - Stopping identity theft.
 - Not allowing false aliases.
 - Creating responsibility/accountability.



The Need

- Sample Scenarios
 - Financial systems
 - Banking transfers, Credit cards, Stock transactions
 - Corporate systems
 - Facility access, Network access, Application access
 - Government programs
 - DMV & Social Security
 - Book of the month club
 - Book reviews and Book questions



Beliefs

- The World is flat
- The Earth is at the center of the Universe
- Biometric data is private

Privacy?

- Biometric Data – Public or Private?
 - Commonly known, easily acquired.
 - Authentication mechanism only.
 - Not able to be changed.
- Handling of Biometric Data
 - Protect from replacement or alteration.
 - Treat like a copyright, not trade secret.
- Use to Protect true Private Elements
 - Accounts, records, transactions, etc.



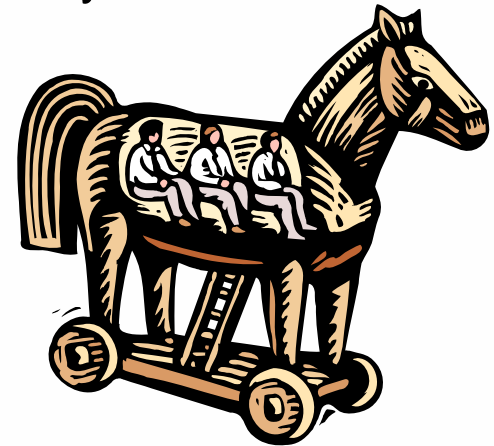
Public Data?

- What is public?
 - “accessible or open to anyone” - Webster's Dictionary
 - Our faces, voices, fingers, and more are commonly seen, recorded, understood.
 - Biometric Data is Public Data, used to authenticate for Private data or transactions.
- How to use Public Data for Secure Authentication?
 - That is what this session is about!



Forms of Attack

- Digital Attacks are
 - Very likely to occur, due to ease and animosity.
 - Requires no physical presence.
 - Cost effective.
- Forms of digital attacks include
 - Replay of previous authentication.
 - Replacement of data in authentication.
 - Interception of authentication.
 - Go around the system all together (use password).
 - Uphill attacks for penetration.



Forms of Attack

- Physical Attacks are
 - Often harder to do.
 - Require physical presence.
 - Good for facility access penetration.
- Forms of physical attacks include
 - False fingers, such as silicon or gummy.
 - Severed fingers, etc photo's.
 - Going around/breaking the system entirely.

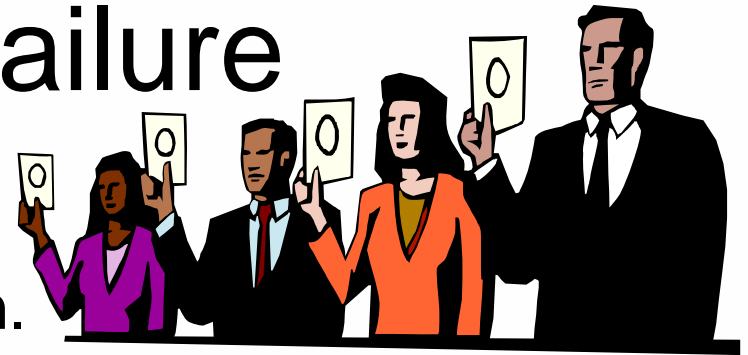


Forms of Attack

- Social Engineering Attacks are
 - Subversive attempts at the system.
 - Ways to use the systems people against it.
 - Cheap and often very effective.
- Forms of social engineering attacks include
 - Phone calls.
 - Site visits.
 - Forms of piggy-backing.



Forms of Failure



- False Accept (Match)
 - Simply a ‘wrong’ identification.
 - Verification versus Identification impact.
- False Reject (Non-Match)
 - A user ‘Piss-off’ factor.
 - Can encumber a systems usage.
- Failure to Enroll
 - Limits usage across a population.
 - Can effect overall costs and policies.

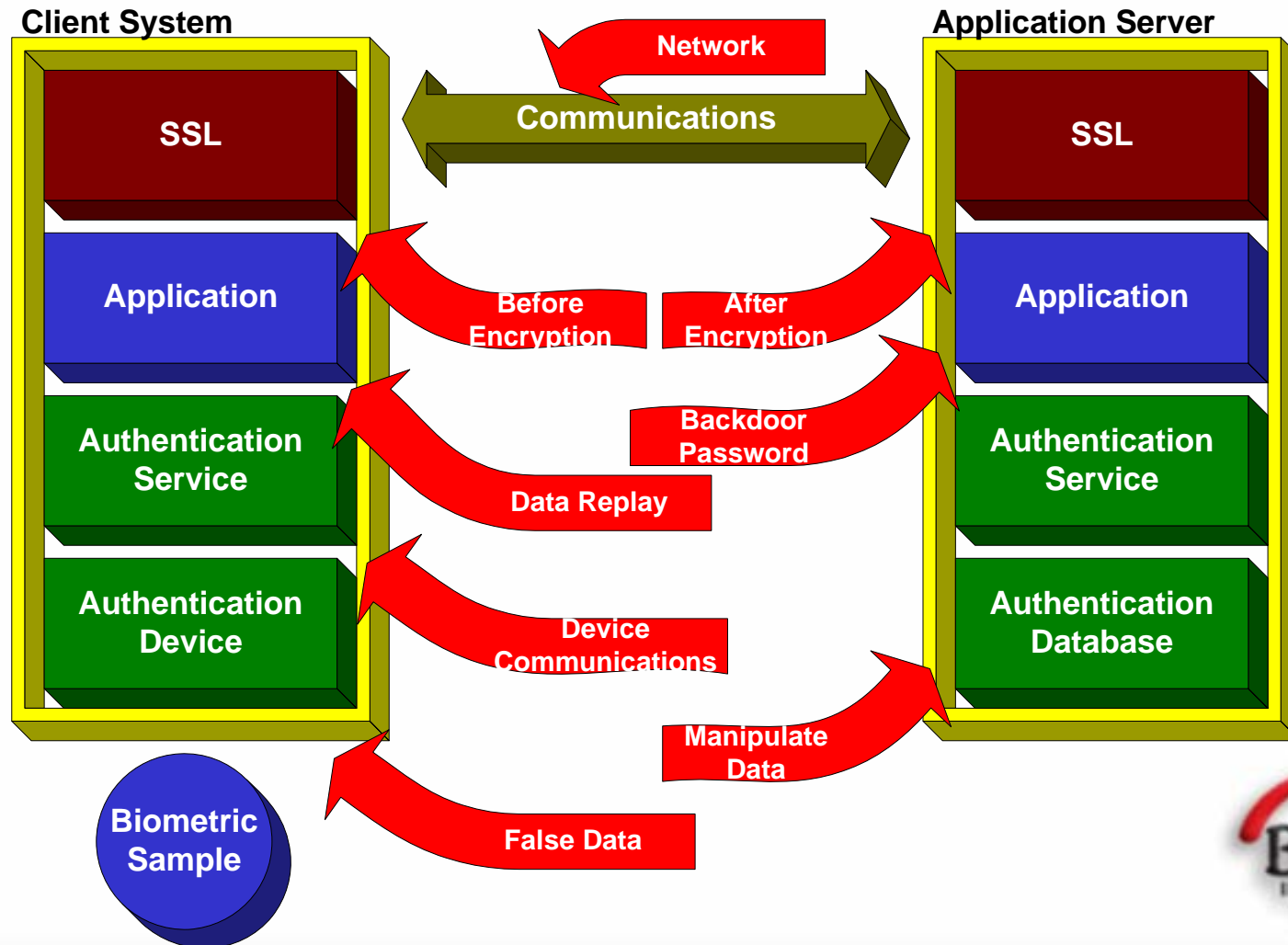
How to Secure Authentication

- Block digital attacks
- Detect and stop physical attacks
- Attain good performance
- Minimize failure of system
- Train users on social engineering

- Sounds easy? Lets see...

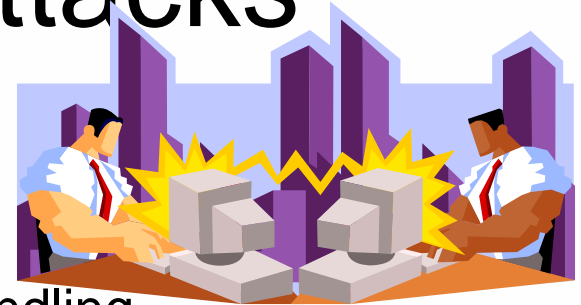


Architecture of Attacks



Stopping Digital Attacks

- Protect communications
 - SSL is not enough.
 - PKI style encryption at the point of data handling.
- Maintain control of the transaction
 - Application/server based control, not user based.
 - Provide effective time-outs and session tracking.
 - Pass/Fail only, to stop up-hill attacks.
- Control the Data
 - Encrypt and protect data storage.
 - Have distinct Enrollment templates and ID models.



Stopping Physical Attacks

- Protect the input of data
 - Liveness Detect – is it live or Memorex?
 - Trusted device communications.
- Have processes
 - Prompt user for input of specific biometric.
 - Tie with ‘something you have’ – a card, etc.
 - Tie with ‘something you know’ – a PIN, etc.
- Protect the mechanisms
 - Secure the covers, wires and interfaces.



Stopping Social Engineering

- Train personnel
 - Create awareness for social engineering.
- Incorporate safe guards
 - Turnstiles to prohibit piggybacking.
 - Policies for information dissemination.
 - Apply multiple checks of identity.



Stopping Failures



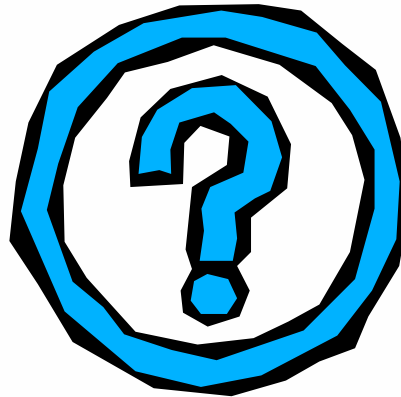
- Achieve high False Accept performance
 - Don't allow any imposters.
 - Generally accuracy in the millions is required.
- Achieve high False Reject performance
 - Keep the users happy and using the system.
 - Must be only a couple of percent at most.
- Have acceptable Failure to Enroll
 - Must use nearly full populations.
 - Each alternate case is a security risk or cost.

Conclusion

- There are many avenues of attack
- There are many elements to secure
- We must
 - Ask the right questions.
 - Determine application levels of risk.
 - Make effective decisions.



Questions?



Mira LaCous

VP Technology and Development

BIO-key International, Inc.

Mira.LaCous@bio-key.com

651-789-6117

