Trust Bubble: A Secure and Privacy-Preserving Framework for Data and Personnel Sharing in Diverse Health Networks

Josephine Lamp[1], Robert Greenes, MD, PhD[1], Edward Shortliffe, MD, PhD[1]

[1]Department of Biomedical Informatics, Arizona State University, Scottsdale, AZ

Abstract

- *Over the last 10+ years, healthcare has been shifting towards more integrated, comprehensive care for the patient*
  - *E.g., Patient Centered Medical Homes and Accountable Care Organizations*
- *Health information exchange and the sharing of data are pertinent*
- *Security and privacy concerns are some of the biggest barriers to adoption of such systems*
- *In order to solve some of these barriers, we present the development of a novel trust framework:*
  - *Framework synthesizes the security measures necessary to support the movement of medical personnel, devices and data between organizations*
  - *Uses organizational policies, risk evaluation techniques and a learning, autonomous trust evaluation mechanism*
  - *Provides adaptive authorization and authentication measures tailored to users and organizational preferences*

Introduction

- Healthcare has been increasingly shifting towards integrated health paradigms [1]
- Within formal integrated health networks, the movement of patients, medical personnel and data is necessary to providing optimal care [3]
- Security and privacy concerns are some of the most challenging barriers preventing successful adoption of health networks [2]
- Previous work on securing health networks has focused on specific security measures for biomedical devices, EHRs or information systems [4, 5]
  - No large-scale methodology to allow for secure inter-organizational movement and communication has been developed
- We present the development of a trust framework that autonomously mediates the access and authentication of personnel, devices and data between organizations based on organizational policies, access history, and determined risk of the entity requesting access

Framework Description

- When a number of entities communicate in an unknown environment, *trust* establishes secure communications between two specific entities
- *Trust Bubble* establishes trust between an external entity and an organizational resource using an autonomous trust evaluation mechanism
- The mechanism determines an entity's risk level, and using the organizational access policy, determines permissions and the level of authentication needed to gain access
- Authentication measures for the entity may be adapted over time
  - The more trusted the entity is, the fewer authentication measures are required

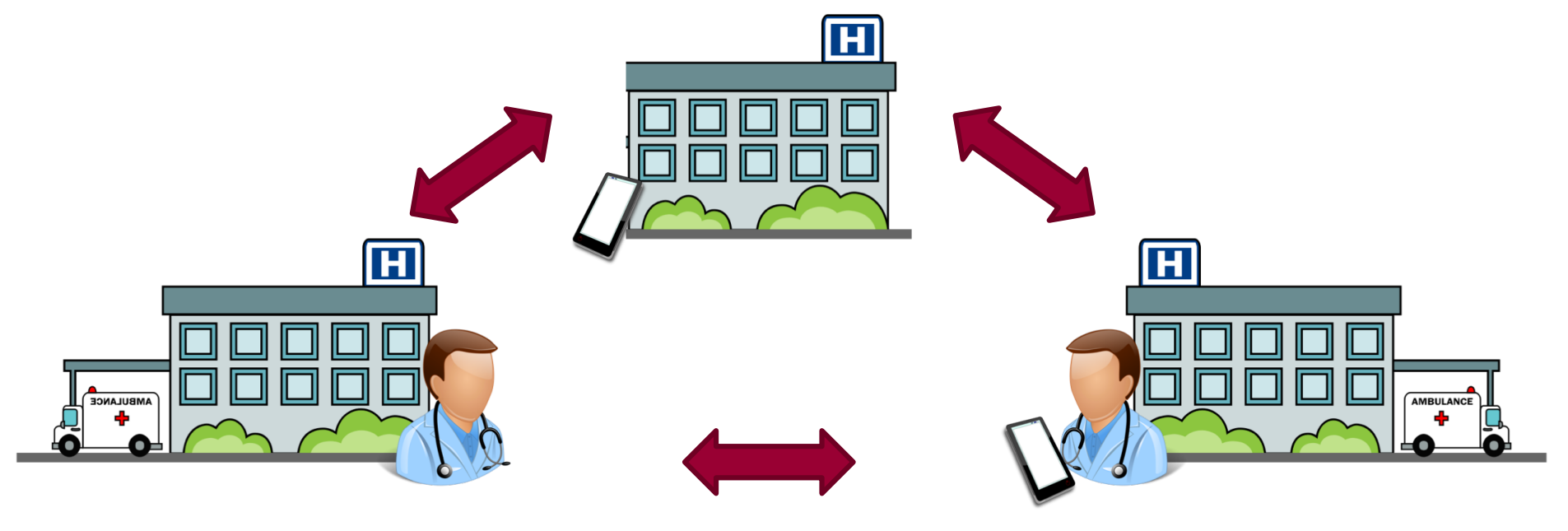


Figure 1. Within a health network, *Trust Bubble* allows for the secure connection and communication of medical personnel, patients and data as they move between organizations.

Trust Bubble Overview

Within a health network, *Trust Bubble* evaluates trust between an external entity and an organization in the following steps, illustrated in Figure 2:

1. An external entity requests access to an organizational resource
2. Using a set of risk factors related to the entity's characteristics and access history (explained in greater detail below,) the risk level of the entity is determined
3. Based on the risk level, the organizational access policy is used to determine the set of permissions and level of authentication needed to grant access for the entity within that organization
4. Adaptive authentication is dynamically invoked, and if the entity successfully completes the authentication request, access is granted
5. Over time, as the entity may become more trusted, less authentication measures may be required for the entity to access the organization's resources

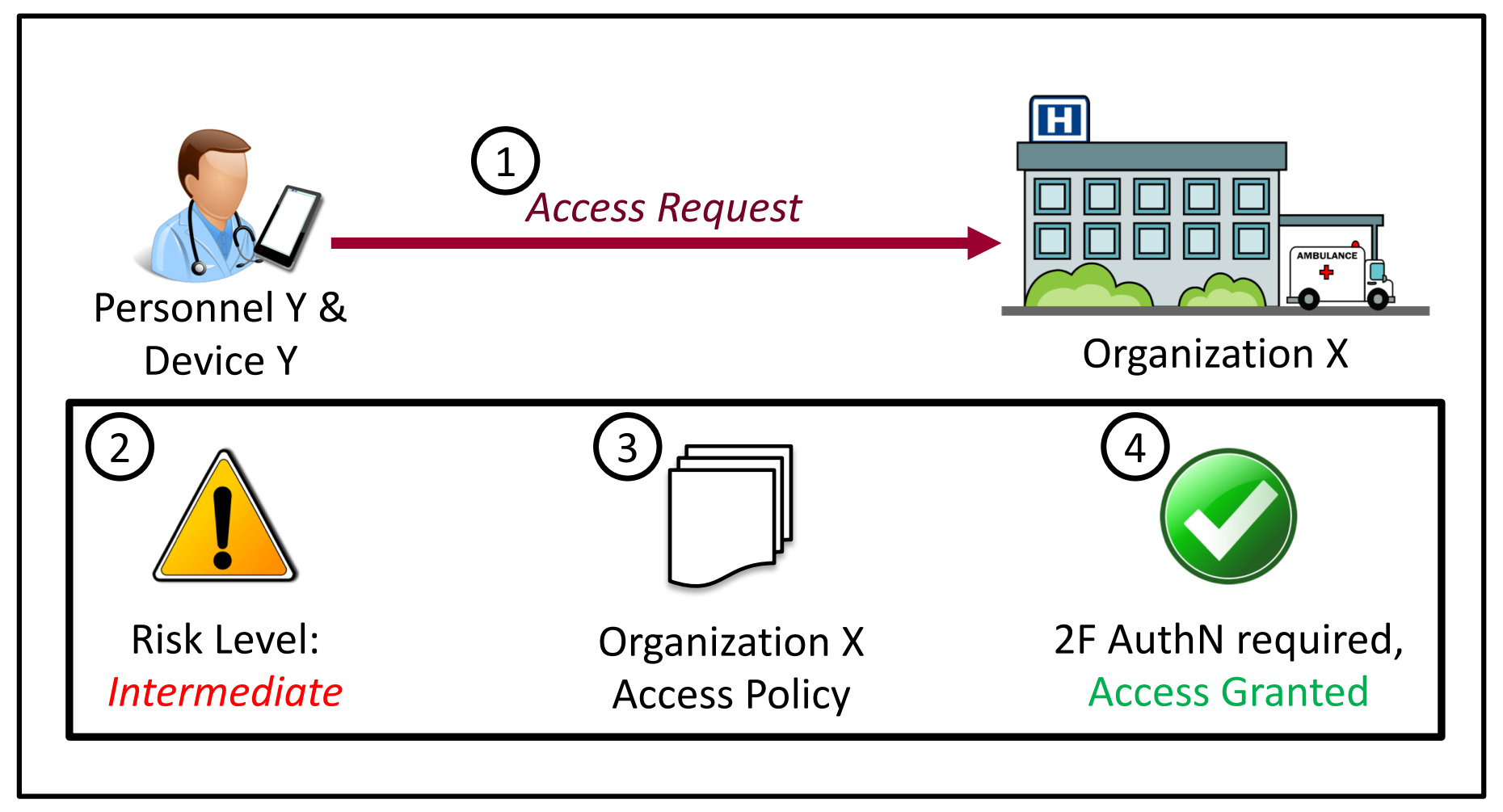

1
Access Request
Personnel Y & Device Y
Organization X
2
Risk Level: *Intermediate*
3
Organization X Access Policy
4
2F AuthN required, Access Granted

Figure 2. The *Trust Bubble* trust evaluation steps.

Risk Determination

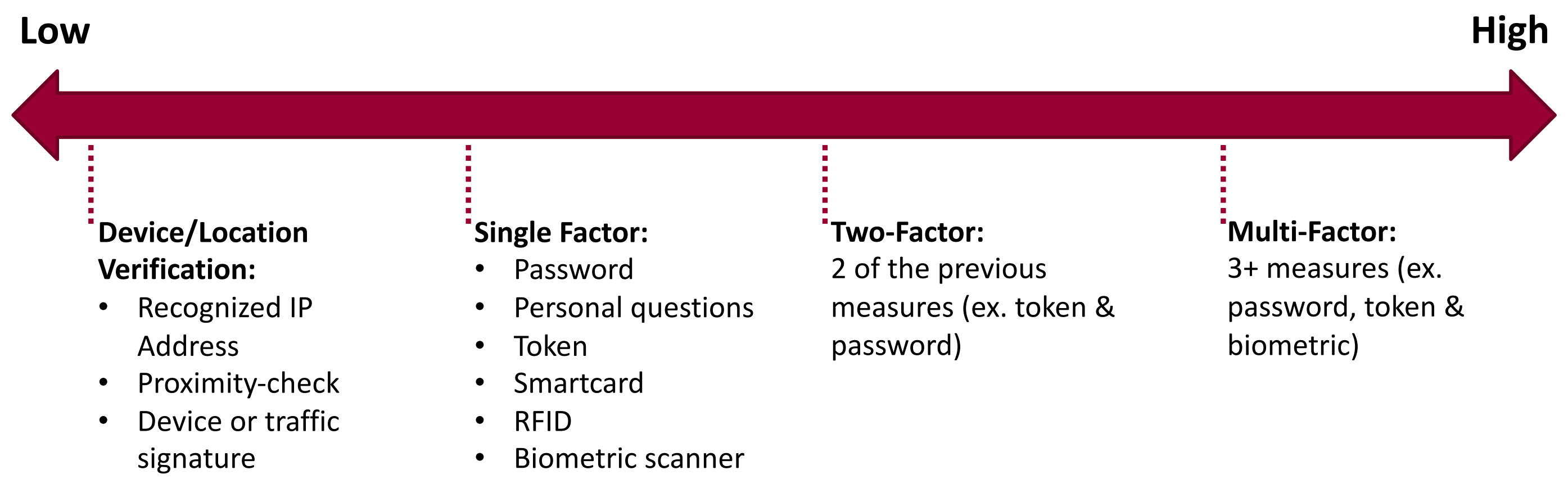
- Risk is determined based on a set of factors explained in Table 1
- The factors are added together for a maximum score of 60 points; higher scores indicate more risk, and lower scores indicate less risk
- The weighting of factors is determined based on organizational preferences
  - For example, an organization that considers all factors of equal importance may use an equal weighting scale as shown in Table 1

Factor	Meaning	Example	Evaluated By	Example Scale
Data Sensitivity	How sensitive the data request may be	Patient identifiable information more sensitive than anonymized data	Data Type (Patient, Anonymized, Public)	0 – 10 (Least – Most Sensitive)
Request Validity	Does the access request make sense for the entity requesting it	A diabetes pump requesting to send commands to an x-ray would not be valid	Comparing entity access rights in policy and access request	0 – 10 (Valid – Not Valid)
Historical Context	Past risk and issues the entity may have caused	Engaging in risky behaviors once accessed in the past	Using past risk scores and audit logs	Past Risk Score ÷ 6 for Scale of 0 – 10 (Not Risky – Risky)
Device Origin	Originating organization device from	Some organizations may be trusted more than others	Organization trust level	0 – 10 (Most – Least Trusted)
Worst-Case Outcome	Outcome upon compromise	Risk to Patient safety, or Confidentiality	Security principle impacted	0 – 10 (Least – Most Important)
Assessment of Security Features	Evaluation of security features implemented	Encryption, basic authentication measures, valid ID or IP address etc.	Security features and implementation levels	0 – 10 (Most – Least Security Implemented)

Table 1. Risk factors used in determining entity risk levels.

Adaptive Authentication

- The level of authentication needed is dynamically determined based on an entity's risk level and history of accesses
- As an entity is determined to be less risky to an organization, fewer authentication measures may be required
- In Emergency situations, an entity may still gain access to organizational resources, but the maximum number of authentication measures may be required (such as multi-factor authentication)



Low

High

Device/Location Verification:
- Recognized IP Address
- Proximity-check
- Device or traffic signature

Single Factor:
- Password
- Personal questions
- Token
- Smartcard
- RFID
- Biometric scanner

Two-Factor:
2 of the previous measures (ex. token & password)

Multi-Factor:
3+ measures (ex. password, token & biometric)

Figure 3. Authentication scale for low to high levels of authentication.

For More Information

For more information, please contact Josephine Lamp at jl4rj@virginia.edu.
Josephinelamp.com

Department of Biomedical Informatics
Arizona State University

Example Use Case

- Organization X is a medium-sized hospital within Health Network Z
- They are concerned about data confidentiality, entity access history and security mechanisms
- Organization X develops the following risk weights for their organizational risk determination:

Factor	Organization X Scale
Data Sensitivity	0 – 20 (Least – Most Sensitive)
Request Validity	0 – 1 (Valid or Not Valid)
Historical Context	0 – 20 (Not Risky – Risky)
Device Origin	0 – 4 (Most – Least Trusted)
Worst-Case Outcome	0 – 5 (Least – Most Important)
Assessment of Security Features	0 – 10 (Most – Least Security Implemented)

Table 2. Organization X's Risk Determination Weighting

- Organization X develops an access policy based on their risk scale summarized in the following table:

Risk Level	Authentication Required	Set of Permissions for Organization X Network
0 – 5 *(Minimal)*	Location Verification	Read, write, send and receive data
6 – 10 *(Low)*	Device Verification	Read, write, send and receive data
11 – 25 *(Fair)*	Single Factor	Read, send and receive data
26 – 45 (*Intermediate)*	Two-Factor	Read and receive data
46 – 60 *(High)*	Multi-Factor	Read data

Table 3. Organization X's Summarized Access Policy

Conclusion

- *Trust Bubble* is a security and privacy-preserving framework
- Overcomes challenges when securing integrated health networks
- Autonomously mediates authorization and authentication of entities to organizational resources
  - Policies and risk scores based on entity characteristics and access history
- Over time, with trust, required organizational resources may be reduced

References

1. American Hospital Association. 2010 Committee on Research. AHA Research Synthesis Report: Patient-Centered Medical Home (PCMH). Chicago: American Hospital Association, 2010.
2. Elmaghraby AS, Losavio MM. Cyber security challenges in smart cities: Safety, security and privacy. J Adv Res [Internet]. Cairo University; 2014;5(4):491–7. Available from: http://dx.doi.org/10.1016/j.jare.2014.02.006
3. Health Care Industry Cybersecurity Task Force. Report on Improving Cybersecurity in the Health Care Industry. 2017;(June):1–88. Available from: https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf
4. Huang Q, Wang L, Yang Y. Secure and Privacy-Preserving Data Sharing and Collaboration in Mobile Healthcare Social Networks of Smart Cities. Secur Commun Networks [Internet]. 2017;2017:1–12. Available from: https://www.hindawi.com/journals/scn/2017/6426495/
5. Kocabas O, Soyata T, Aktas MK. Emerging Security Mechanisms for Medical Cyber Physical Systems. IEEE/ACM Trans Comput Biol Bioinforma. 2016;13(3):401–16.