USC Viterbi
School of Engineering

Context-Aware Security

Jiaqi Ma && Mo Zhang

Nov 9, 2022

Traditional Static Approaches:

- Separate networks
- New Saas application
- VPN access
- The threat landscape outside
- Own devices (BYOD)
- ……

Security is based on siloed yes/no decisions.

Dynamic Security Decisions:

who, what, when, where and why of access

It increases both security and user productivity.

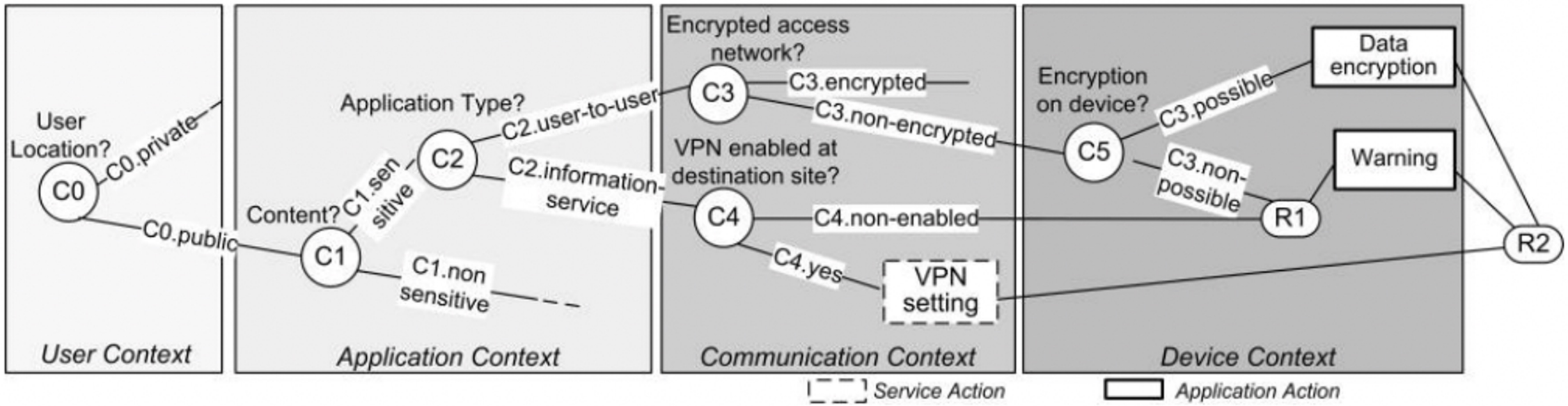
Context-Aware Security: an adaptive model

- make real-time security decisions on the total risk associated with multiple pieces of security information
- change security from “you have access to everything when you login” to “you’ll have access to some things based on where you are and what you’re trying to do, on what device and at what time”

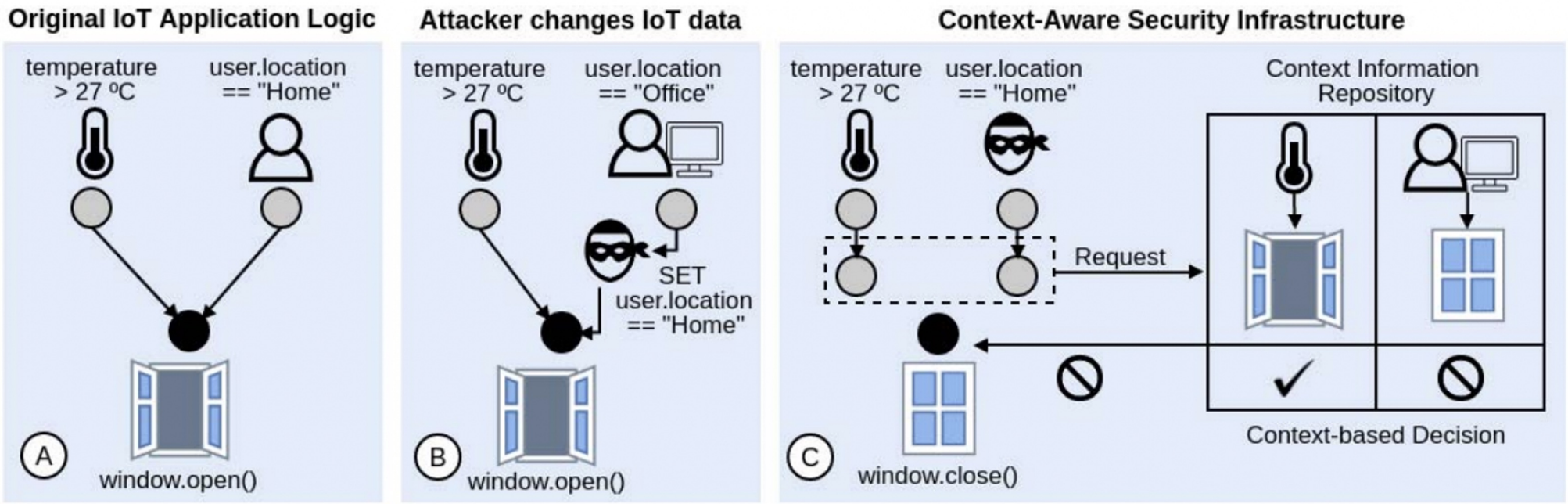
The Security Analytics Engine:

One context-aware model implements a security analytics engine that returns a risk score based on multiple factors like:

- Browser used: historical analysis of any browser use that falls outside of normal behavior
- Location pattern: abnormal location
- Specific location: specific locations or geographies known to foster malicious activity
- Time: outside of customary times and days
- Blacklist: a list of forbidden networks or network addresses
- Whitelist: a list of approved networks or network addresses


User Location?
C0
C0.private
C0.public
User Context
Content?
C1
C1.sen sitive
C1.non sensitive
Application Type?
C2
C2.user-to-user
C2.information-service
Application Context
Encrypted access network?
C3
C3.encrypted
C3.non-encrypted
VPN enabled at destination site?
C4
C4.non-enabled
C4.yes
VPN setting
Communication Context
Encryption on device?
C5
C3.possible
C3.non-possible
Data encryption
Warning
R1
R2
Device Context
Service Action
Application Action

Example:


Original IoT Application Logic
temperature
> 27 ºC
user.location
== "Home"
A
window.open()
Attacker changes IoT data
temperature
> 27 ºC
user.location
== "Office"
SET
user.location
== "Home"
B
window.open()
Context-Aware Security Infrastructure
temperature
> 27 ºC
user.location
== "Home"
Request
Context Information
Repository
C
window.close()
Context-based Decision

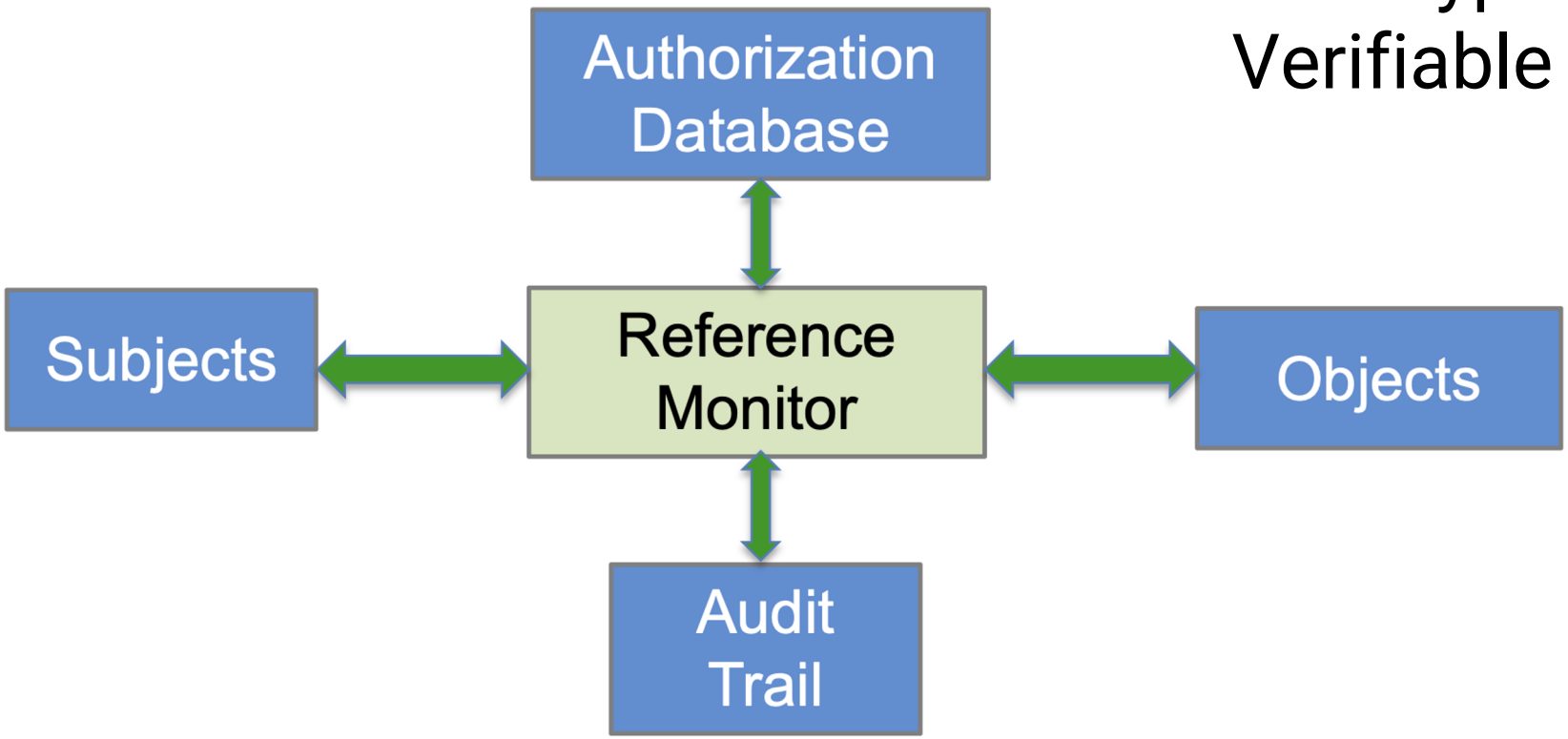

IAM
Firewall
Monitoring
Security Analytics Engine
Edit Policy
policy
risk score
Enforcement
Conditions
thresholds

Example:

Risk Policy	Value
Time	
During normal work hours	0
Outside normal work hours	10
Location	
On-premises	0
Remote	10
Device	
Corporate controlled	0
BYOD managed device	5
Unmanaged device	10
Policy threshold	
Sales Manager	25

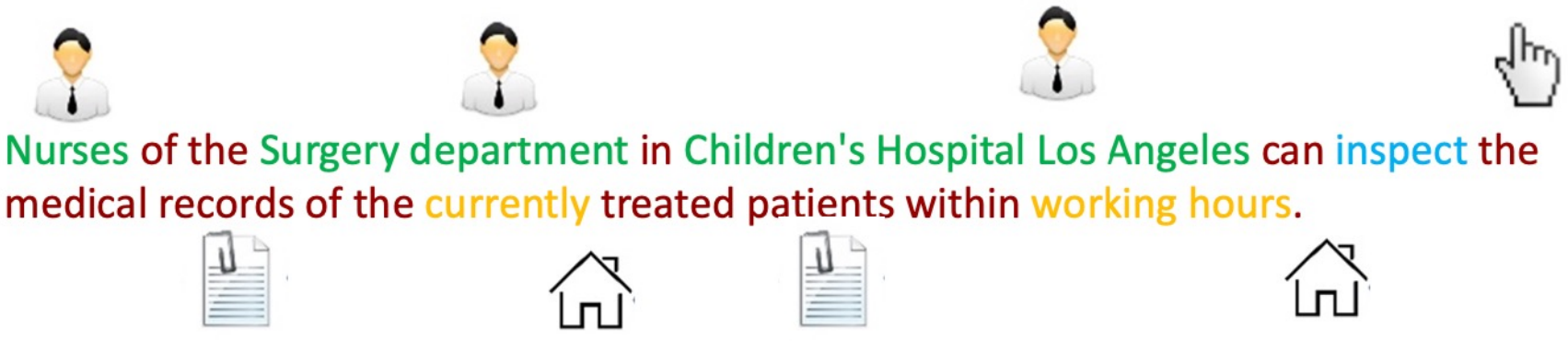
Reference Monitor:

Tamperproof ×
Non-bypassable ×
Verifiable ×



Context-Aware Security v.s. Attribute Based Access Control:

- Dynamic v.s. static
- Threshold/score v.s. yes/no



Advantages:

- increase both security and user productivity
- once setup, reduce security workload
- flexible for management

Limitations:

- need values for risk policy: how to choose values?
- impossible to detect access leakage

References:

- https://www.oneidentity.com/context-aware-security/
- https://atos.net/en/lp/zero-trust-security-magazine/the-power-and-potential-of-context-aware-security
- https://www.linkedin.com/pulse/what-context-aware-security-use-cases-praveen/
- Matteo Bandinelli, Federica Paganelli, Gianluca Vannuccini, Dino Giuli: “A Context-aware Security Framework for Next Generation Mobile Networks”
- Everton de Matos, Ramao Tiago Tiburski, Leonardo Albernaz Amaral, Fabiano Hessel: “Providing Context-Aware Security for IoT Environments Through Context Sharing Feature”