CIS 700/002 : Special Topics : Protection Mechanisms & Secure Design Principles

Nikheel V Savant

CIS 700/002: Security of EMBS/CPS/IoT

Department of Computer and Information Science
School of Engineering and Applied Science
University of Pennsylvania

01/27/2017

Topics to be covered:

- Protection Mechanisms
- Secure Design Principles

Topics to be covered:

- Protection Mechanisms
- Secure Design Principles

Protection Mechanisms

- Authentication
- Access Control
- Firewall
- Intrusion Detection
- Antimalware
- Application Whitelisting
- Flow Whitelisting
- Cryptography
- Integrity Verification
- Survivability

Protection Mechanisms

- Authentication
- Access Control
- Firewall
- Intrusion Detection
- Antimalware
- Application Whitelisting
- Flow Whitelisting
- Cryptography
- Integrity Verification
- Survivability

So what comes to your mind when you hear Authentication???


Password
****

Challenge for selecting appropriate Password

Strong Password

Easy to remember

On the Semantic Patterns of Passwords and their Security Impact

By Veras, R., Collins, C., and Thorpe, J. (2014)

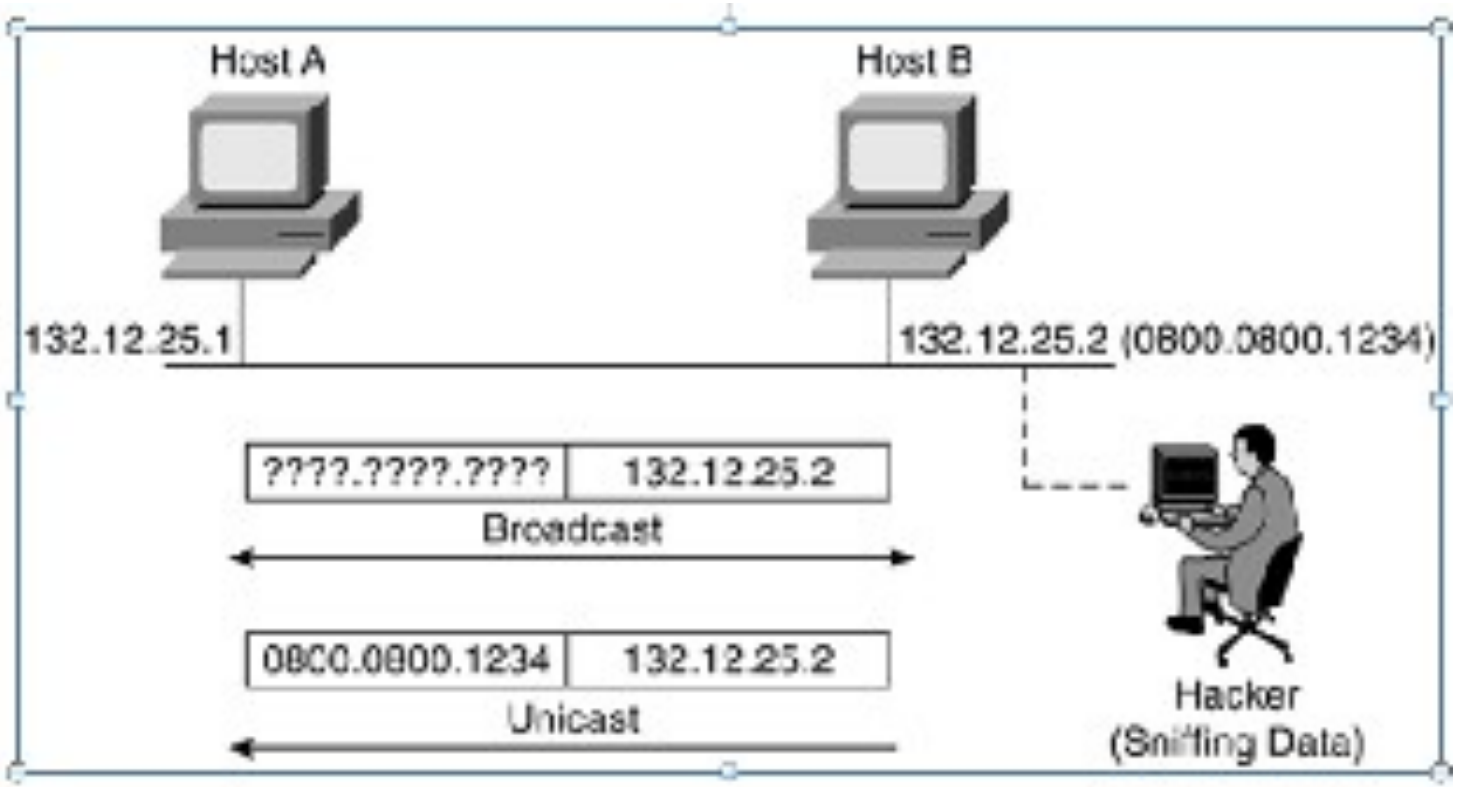
On the Semantic Patterns of Passwords and their Security Impact

Better than the state-of-the-art approach:

In experiments limited to 3 billion guesses

- Guessed ***67%*** more passwords from the LinkedIn leak
- ***32%*** more passwords from the MySpace leak

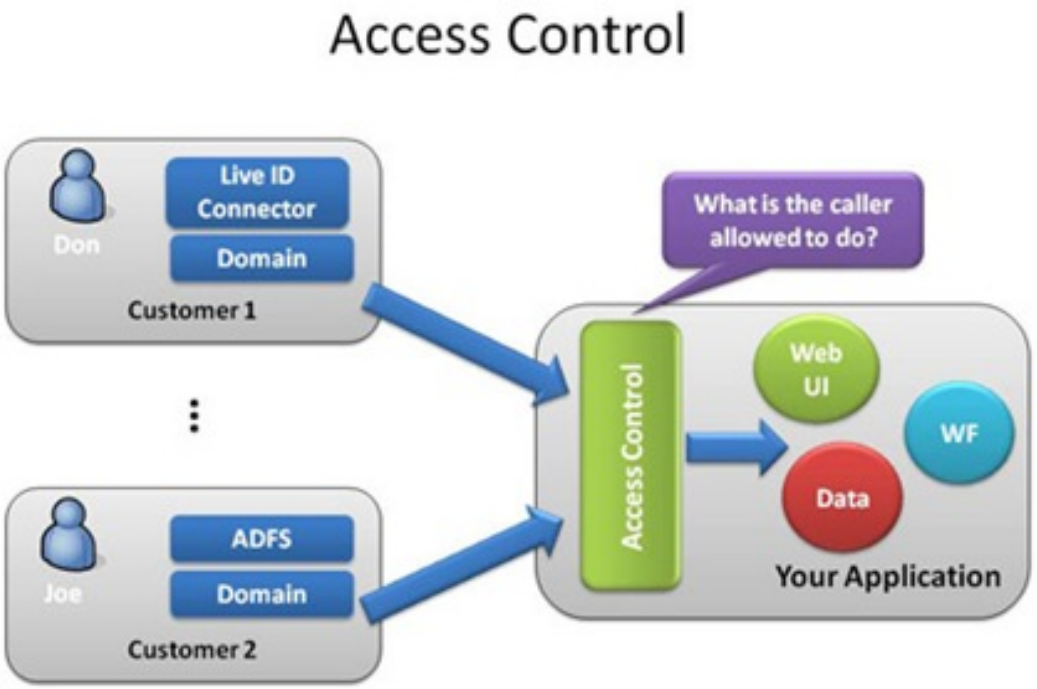
Eavesdropping



Protection Mechanisms

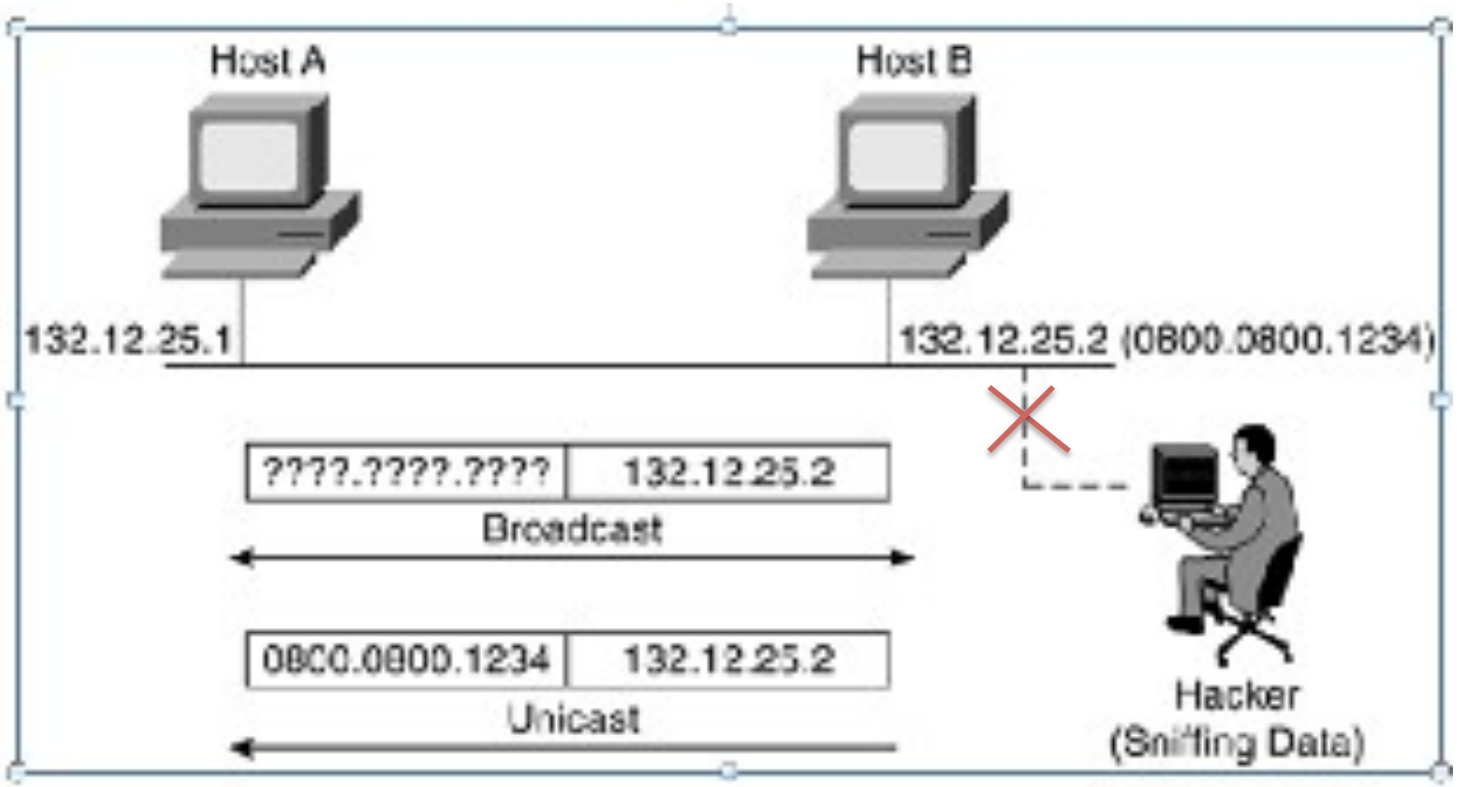
- Authentication
- Access Control
- Firewall
- Intrusion Detection
- Antimalware
- Application Whitelisting
- Flow Whitelisting
- Cryptography
- Integrity Verification
- Survivability

Access Control



Access Control

- Prevents Eavesdropping



Conventional Authentication Factor Challenge-Response Protocol

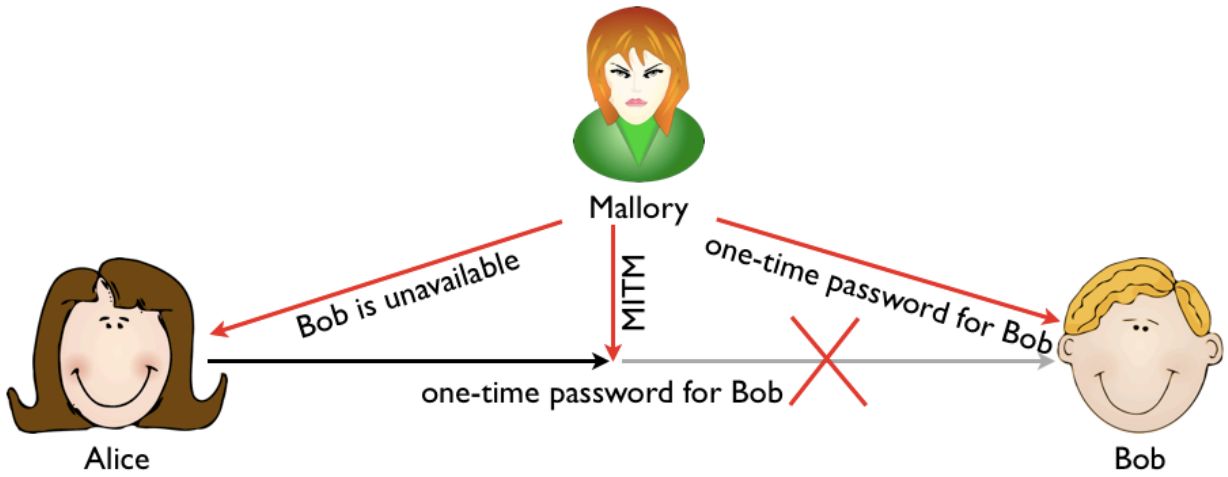
(key)

challenge

F(key, challenge)

(key)

Man-in-the-Middle Attack(MitMA)



Man-in-the-Middle Attack(MitMA)

Alice *"Hi Bob, it's Alice. Give me your key."* → Mallory Bob

Man-in-the-Middle Attack(MitMA)

Alice *"Hi Bob, it's Alice. Give me your key."* → Mallory Bob

Alice Mallory *"Hi Bob, it's Alice. Give me your key."* → Bob

Man-in-the-Middle Attack(MitMA)

Alice *"Hi Bob, it's Alice. Give me your key."* → Mallory Bob

Alice Mallory *"Hi Bob, it's Alice. Give me your key."* → Bob

Alice Mallory ← *[Bob's key]* Bob

Man-in-the-Middle Attack(MitMA)

Alice *"Hi Bob, it's Alice. Give me your key."* → Mallory Bob

Alice Mallory *"Hi Bob, it's Alice. Give me your key."* → Bob

Alice Mallory ← *[Bob's key]* Bob

Alice ← *[Mallory's key]* Mallory Bob

Man-in-the-Middle Attack(MitMA)

Alice *"Hi Bob, it's Alice. Give me your key."* → Mallory Bob

Alice Mallory *"Hi Bob, it's Alice. Give me your key."* → Bob

Alice Mallory ← *[Bob's key]* Bob

Alice ← *[Mallory's key]* Mallory Bob

Alice *"Meet me at the bus stop!" [encr. Mallory's key]* → Mallory Bob

Man-in-the-Middle Attack(MitMA)

Alice *"Hi Bob, it's Alice. Give me your key."* → Mallory Bob

Alice Mallory *"Hi Bob, it's Alice. Give me your key."* → Bob

Alice Mallory ← *[Bob's key]* Bob

Alice ← *[Mallory's key]* Mallory Bob

Alice *"Meet me at the bus stop!" [encr. Mallory's key]* → Mallory Bob

Alice Mallory *"Meet me at the van down by the river!" [Bob's key]* → Bob

Man-in-the-Middle Attack(MitMA)

Alice *"Hi Bob, it's Alice. Give me your key."* → Mallory Bob

Alice Mallory *"Hi Bob, it's Alice. Give me your key."* → Bob

Alice Mallory ← *[Bob's key]* Bob

Alice ← *[Mallory's key]* Mallory Bob

Alice *"Meet me at the bus stop!" [encr. Mallory's key]* → Mallory Bob

Alice Mallory *"Meet me at the van down by the river!" [Bob's key]* → Bob

Bob thinks that this message is a secure communication from Alice

Man-in-the-Middle Attack(MitMA)

Alice *"Hi Bob, it's Alice. Give me your key."* → Mallory Bob

Alice Mallory *"Hi Bob, it's Alice. Give me your key."* → Bob

Alice Mallory ← *[Bob's key]* Bob

Alice ← *[Mallory's key]* Mallory Bob

Alice *"Meet me at the bus stop!" [encr. Mallory's key]* → Mallory Bob

Alice Mallory *"Meet me at the van down by the river!" [Bob's key]* → Bob

Bob thinks that this message is a secure communication from Alice

Bob goes to the van down by the river and gets robbed by Mallory

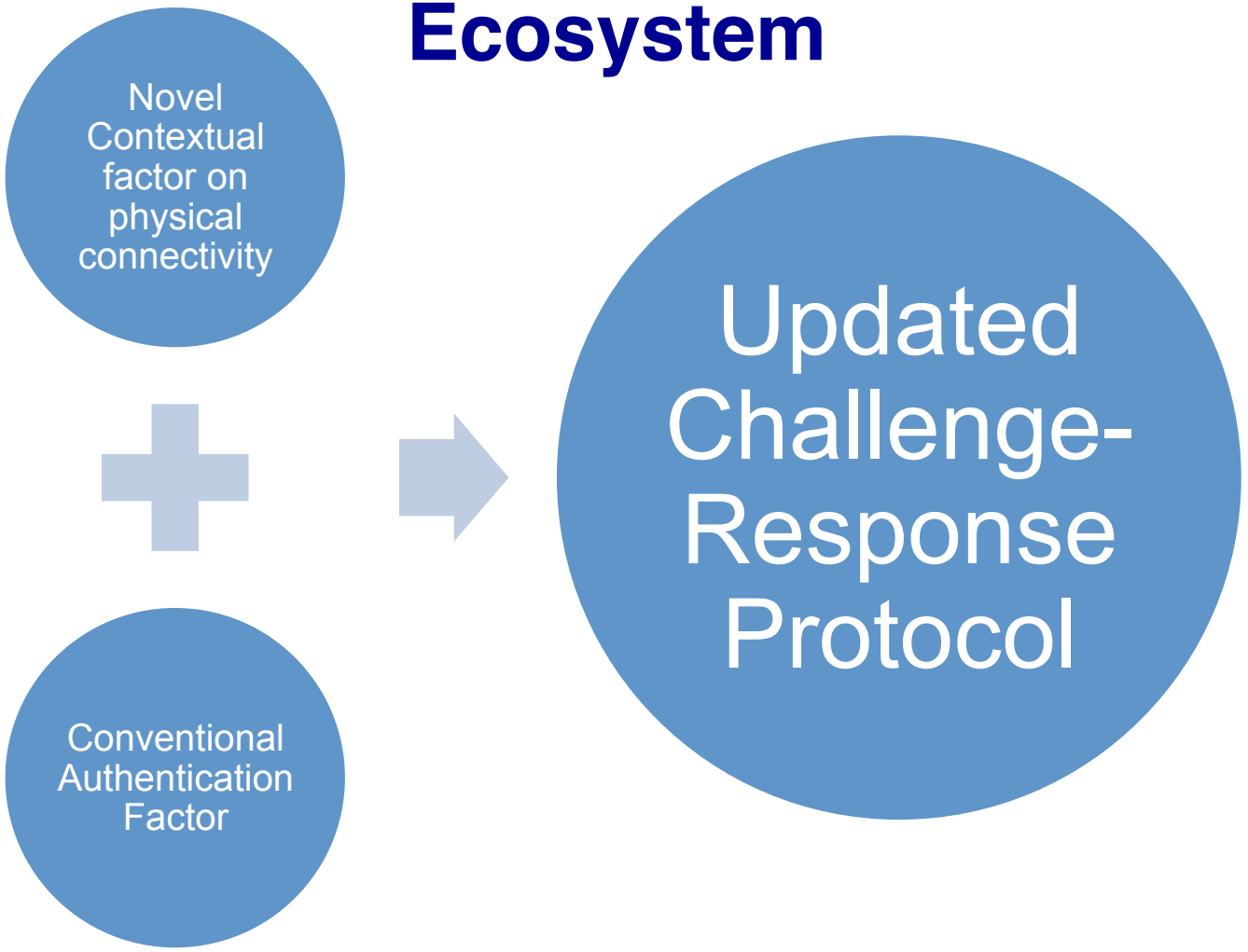
Cyber–Physical Device Authentication for the Smart Grid Electric Vehicle Ecosystem

Aldar C.-F. Chan, Senior Member, IEEE, and Jianying Zhou

Penn Engineering

PRECISE
PENN RESEARCH IN EMBEDDED COMPUTING AND INTEGRATED SYSTEMS ENGINEERING

Cyber–Physical Device Authentication for the Smart Grid Electric Vehicle Ecosystem

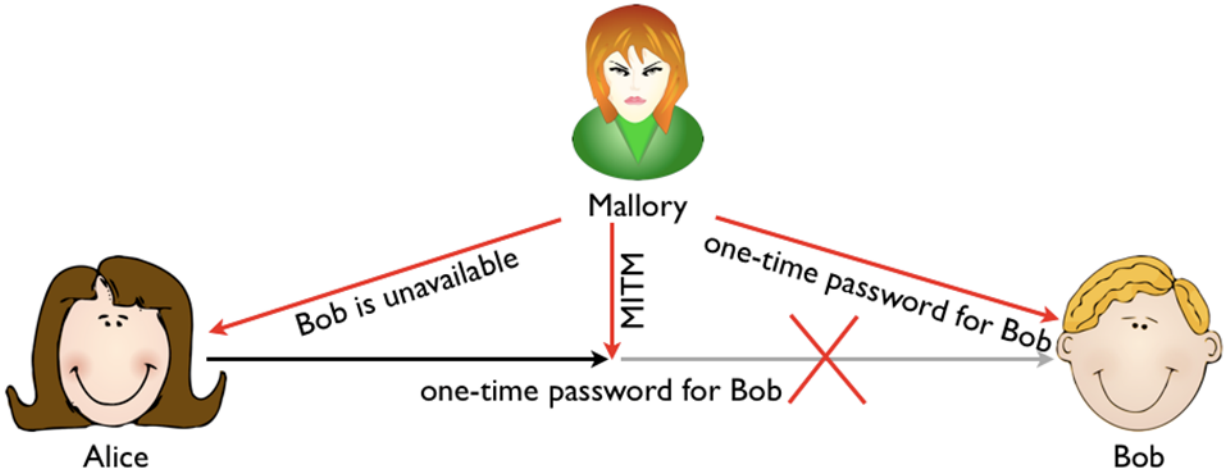


Penn Engineering

PRECISE
PENN RESEARCH IN EMBEDDED COMPUTING AND INTEGRATED SYSTEMS ENGINEERING

Novel Contextual factor on physical connectivity

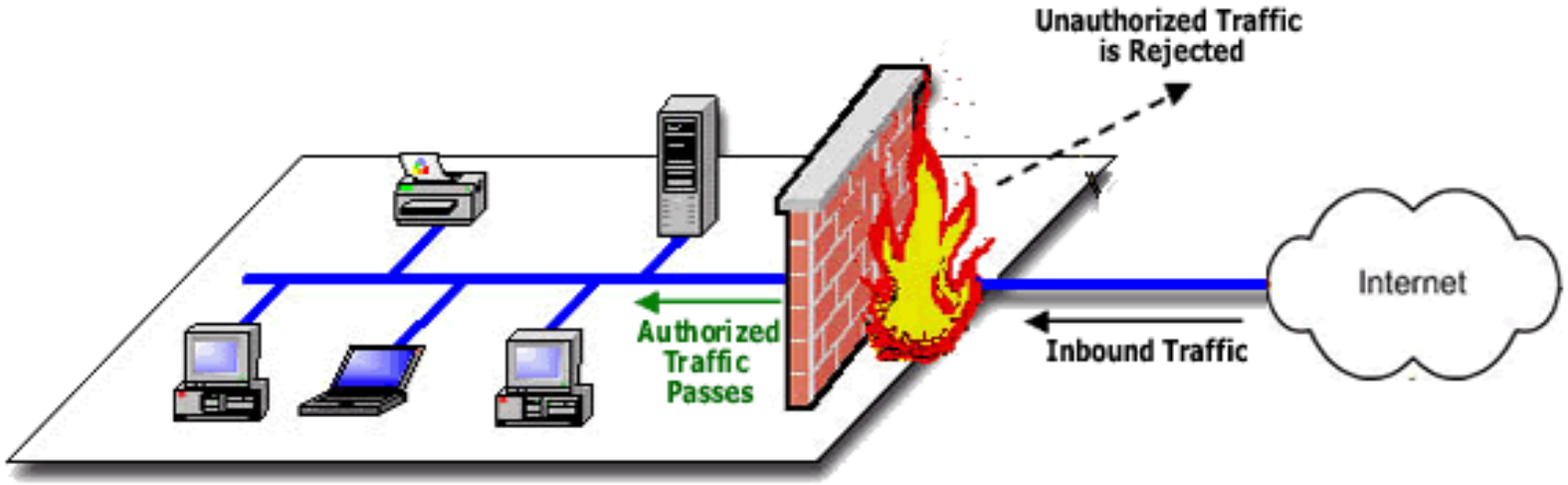
- Latency examination
  - Ex: long cryptographic hash function



Protection Mechanisms

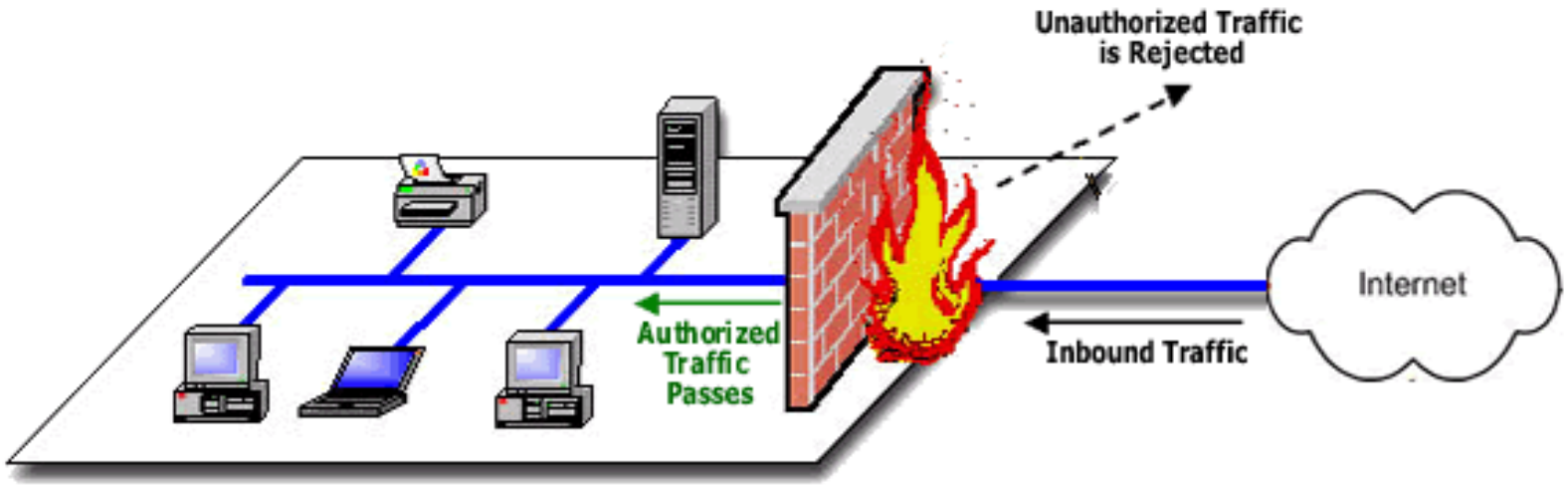
- Authentication
- Access Control
- Firewall
- Intrusion Detection
- Antimalware
- Application Whitelisting
- Flow Whitelisting
- Cryptography
- Integrity Verification
- Survivability

Firewall


Unauthorized Traffic
is Rejected
Internet
Authorized
Traffic
Passes
Inbound Traffic

Firewall

Barriers between the internal network & any other network, such as the Internet.



Firewall

- Upon receiving a network packet, the firewall analyzes its characteristics:
  - Source address,
  - Destination address,
  - port number,
  - network status,
  - actual data delivered, etc

Firewall

- After analysis it determines:
  - whether to let it go through,

Firewall

- After analysis it determines:
  - whether to let it go through,
  - drop it,

Firewall

- After analysis it determines:
  - whether to let it go through,
  - drop it,
  - delay it, or

Firewall

- After analysis it determines:
  - whether to let it go through,
  - drop it,
  - delay it, or
  - redirect it for further inspection

Firewall

Different types of firewalls:

- Simplest and most lightweight form
  - take decisions based on static rules
- Stateful firewalls
  - keep a history of the packets inspected
- Proxy firewalls
  - protect users in the internal network
- Deep packet inspection firewalls
  - take the packets apart, analyze the data they carry, and look for particular content

Firewall

Different types of firewalls:

- Simplest and most lightweight form
  - take decisions based on static rules
- Stateful firewalls
  - keep a history of the packets inspected
- Proxy firewalls
  - protect users in the internal network
- Deep packet inspection firewalls
  - take the packets apart, analyze the data they carry, and look for particular content

Firewall

Different types of firewalls:

- Simplest and most lightweight form
  - take decisions based on static rules
- Stateful firewalls
  - keep a history of the packets inspected
- Proxy firewalls
  - protect users in the internal network
- Deep packet inspection firewalls
  - take the packets apart, analyze the data they carry, and look for particular content

Firewall

Different types of firewalls:

- Simplest and most lightweight form
  - take decisions based on static rules
- Stateful firewalls
  - keep a history of the packets inspected
- Proxy firewalls
  - protect users in the internal network
- Deep packet inspection firewalls
  - take the packets apart, analyze the data they carry, and look for particular content

Firewall Cons

Its effectiveness is only as good as its configuration.

Trends in Firewall Config. Errors

Measuring the Holes in Swiss Cheese

Avishai Wool(2010)

Protection Mechanisms

- Authentication
- Access Control
- Firewall
- Intrusion Detection
- Antimalware
- Application Whitelisting
- Flow Whitelisting
- Cryptography
- Integrity Verification
- Survivability

Intrusion Detection

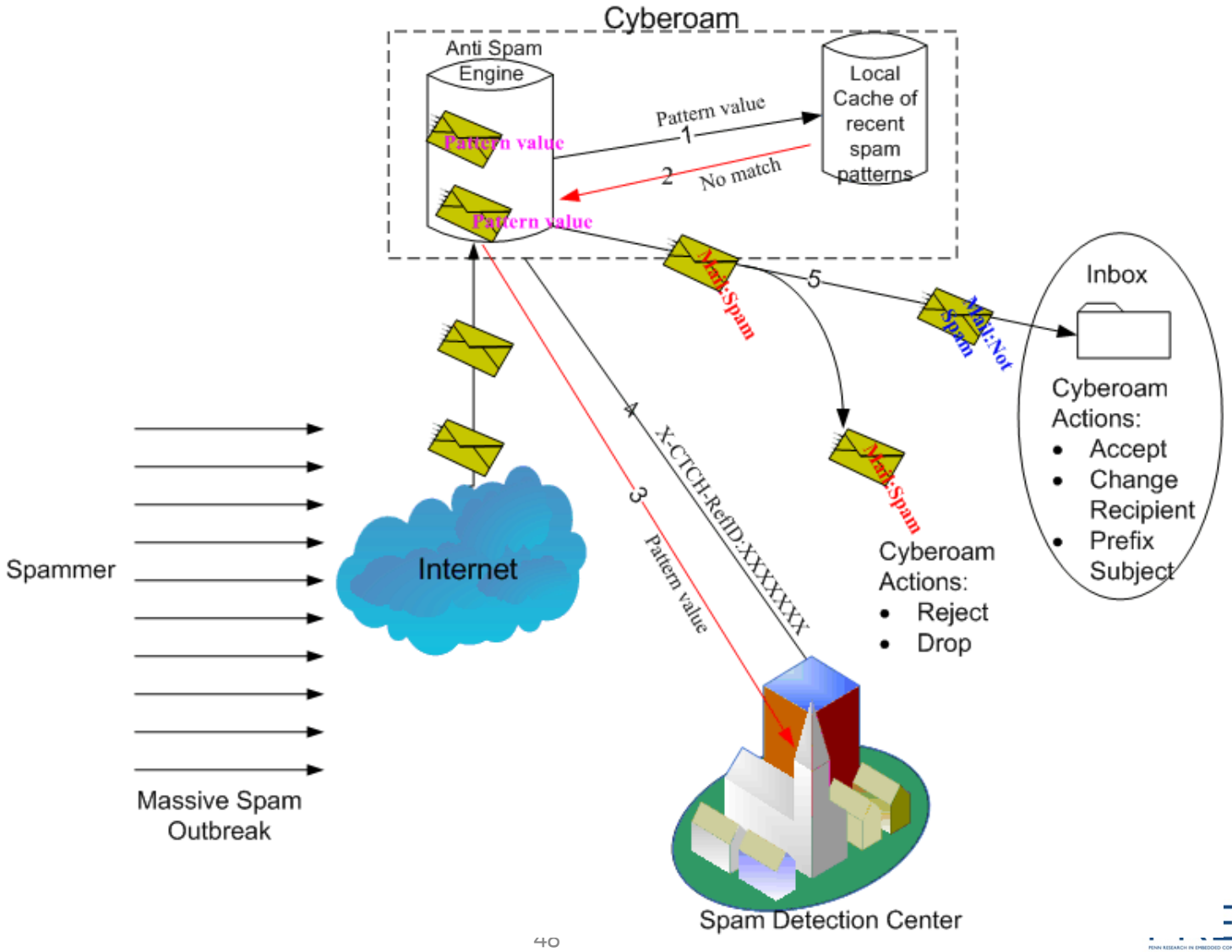
Intrusion Detection

- Monitors a network or systems for malicious activity or policy violations.
- Uses alarm filtering techniques to distinguish malicious activity from false alarms.
  - Ex: antivirus software

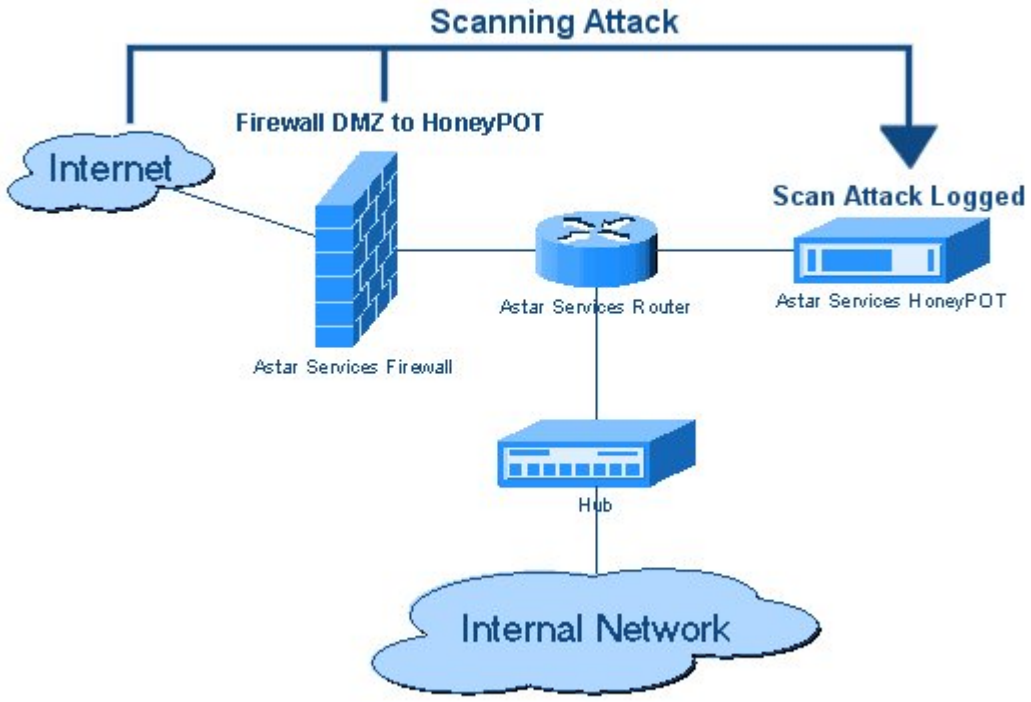
Intrusion Detection Mechanisms

- Knowledge-based:
  - referred to as pattern-based,
  - signature-based, or
  - misuse detection
- Behavior-based:
  - referred to as anomaly-based detection

Knowledge-based Intuition detection



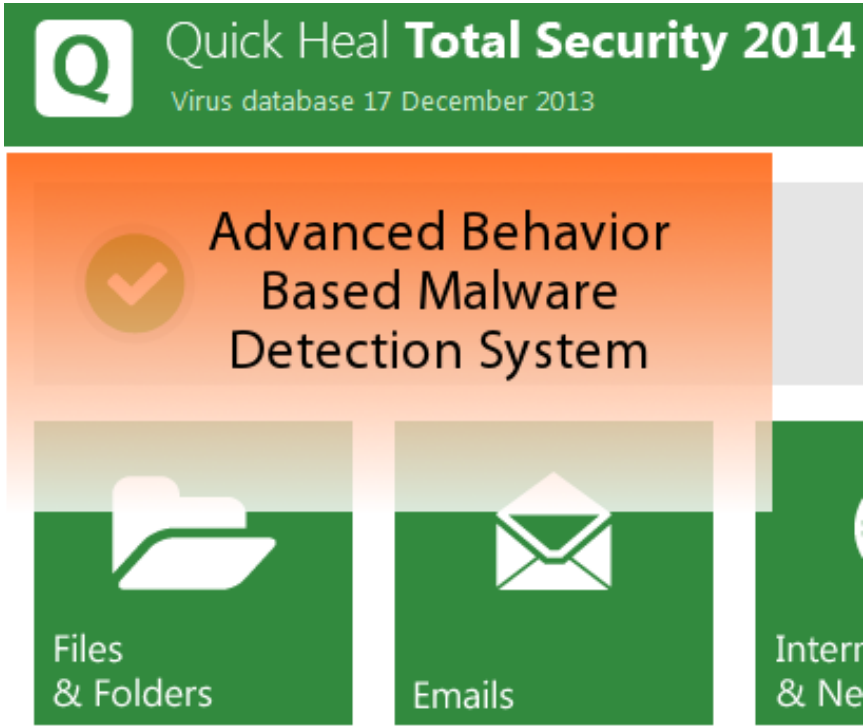
Training approach(Honeypot)



Intrusion Detection Mechanisms

- Knowledge-based:
  - referred to as pattern-based,
  - signature-based, or
  - misuse detection
- Behavior-based:
  - referred to as anomaly-based detection

Behavior-based Intuition detection



Behavior-based Intuition detection

- Better at detecting attacks that have not been previously observed.

- They work by first defining what behavior should be considered as ordinary for a particular system and by then looking for evidence of behavior that is out of the ordinary.

Behavior-based Intuition detection

- Better at detecting attacks that have not been previously observed.

- They work by first defining what behavior should be considered as ordinary for a particular system and by then looking for evidence of behavior that is out of the ordinary.

Intrusion Detection Mechanisms

- Knowledge-based

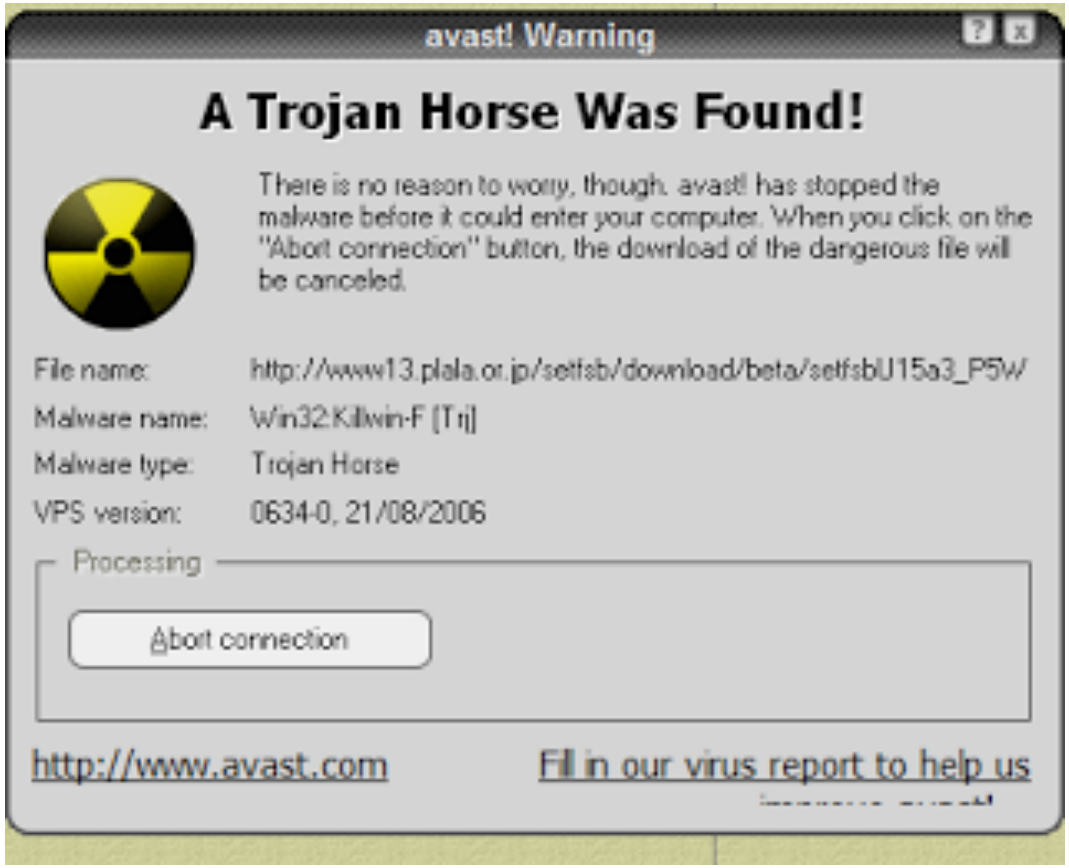
- Behavior-based

Malware

Software used to disrupt computer or mobile operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising

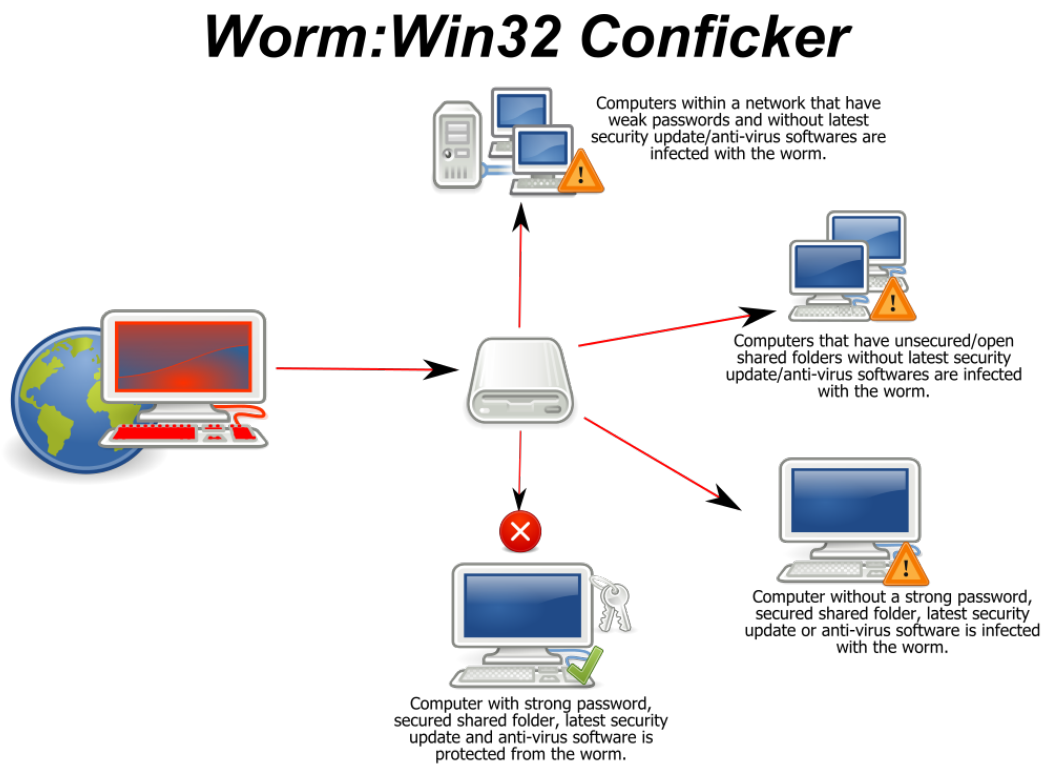
Trojans

Any malicious computer program which is used to hack into a computer by misleading users of its true intent



Worms

Program that replicates itself in order to spread to other computers.



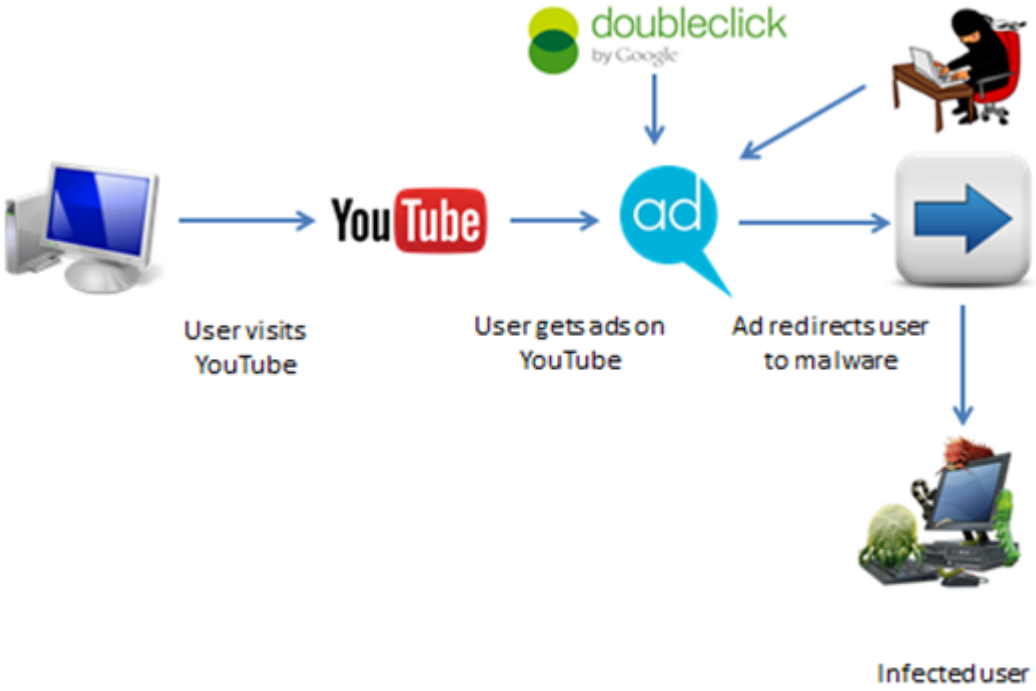
Conficker Worm

Backdoors

Software by the programmer who created the original program and is often only known to that person

Exploits

Software, data, or commands to "**exploit**" a weakness in a computer system or program to carry out some form of malicious intent, such as a denial-of-service attack, Trojan horses, worms or viruses

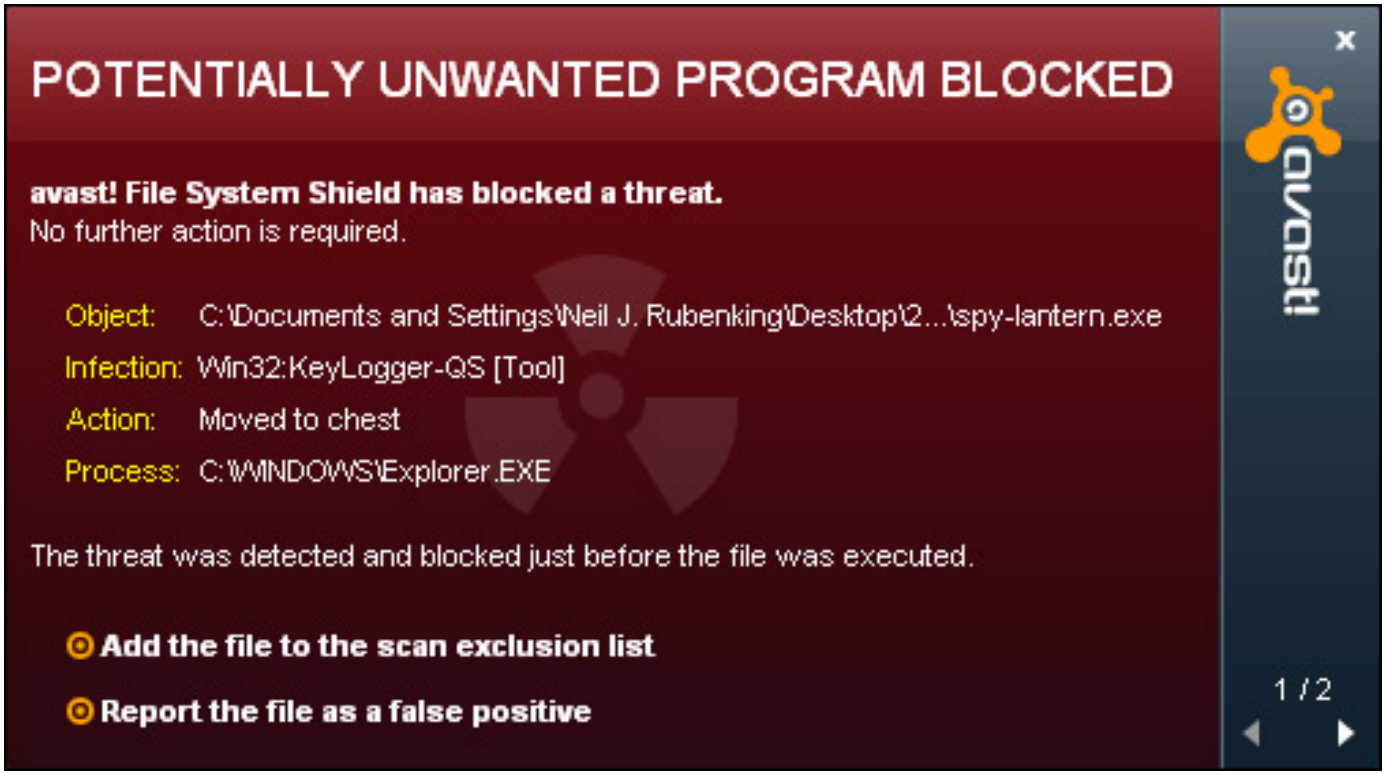


Adware

A program that may be unwanted, despite the possibility that users consented to download it

PUP (Potentially Unwanted Programs)

A program that may be unwanted, despite the possibility that users consented to download it.



Social Engineering

An attack vector that relies heavily on human interaction and often involves tricking people into breaking normal security procedures.

Popular Social Engineering

- Phishing
- Scareware

Phishing(Fishing + Phreaking)

When a malicious party sends a fraudulent email disguised as a legitimate email, often purporting to be from a trusted source.

Scareware

Tricking the victim into thinking his computer is infected with malware and trick to buy him software such as fake antivirus protection.

Protection Mechanisms

- Authentication
- Access Control
- Firewall
- Intrusion Detection
- Antimalware
- Application Whitelisting
- Flow Whitelisting
- Cryptography
- Integrity Verification
- Survivability

Antimalware

Antimalware

A program of awareness for malware and social engineering, using similar concept as knowledge-based intrusion detection systems.

Guide to Malware Incident Prevention and Handling for Desktops and Laptops

By Murugiah Souppaya, Karen Scarfone

Guide to Malware Incident Prevention and Handling for Desktops and Laptops

- Malware Incident Prevention
- Malware Incident Response

Malware Incident Prevention

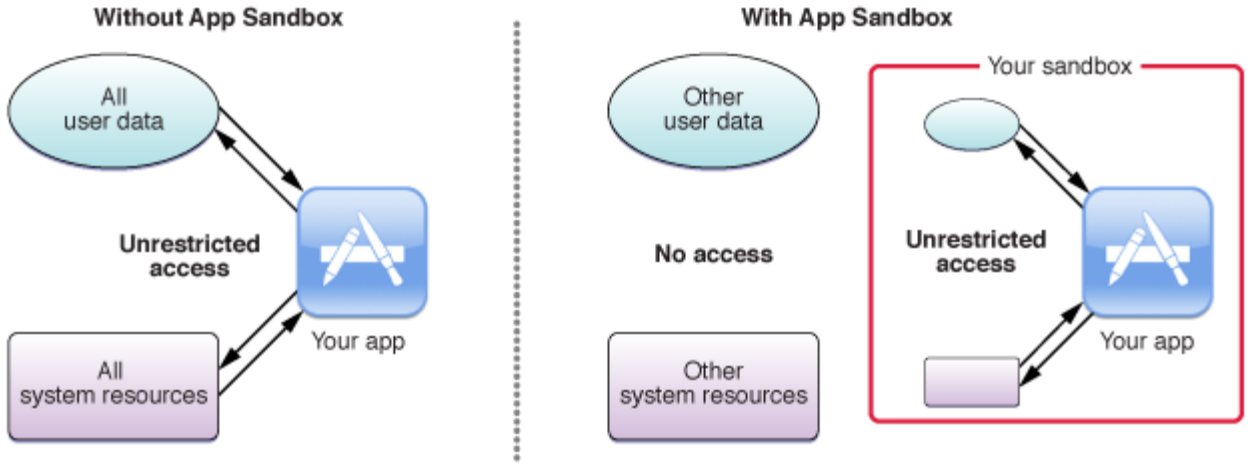
- Antivirus Software
- Firewalls
- Sandboxing

Malware Incident Prevention

- Antivirus Software
- Firewalls
- Sandboxing
  - It is often used to execute untested or untrusted programs or code, possibly from unverified or untrusted third parties, suppliers, users or websites, without risking harm to the host machine

Malware Incident Prevention

- Antivirus Software
- Firewalls
- Sandboxing



Malware Incident Response

- Building and Maintaining Malware-Related Skills
- Facilitating Communication and Coordination

Detecting Malicious Software Execution in Programmable Logic Controllers Using Power Fingerprinting

By Carlos Aguayo, Alan Hinton

Using power consumption patterns

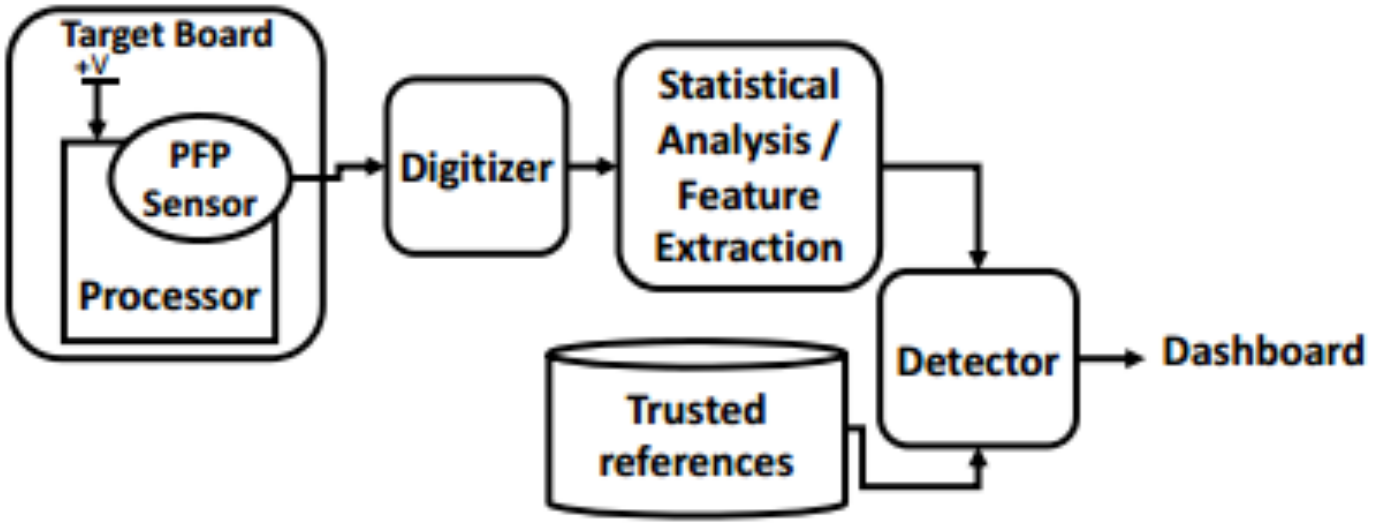
Detecting Malicious Software Execution in Programmable Logic Controllers Using Power Fingerprinting

By Carlos Aguayo, Alan Hinton

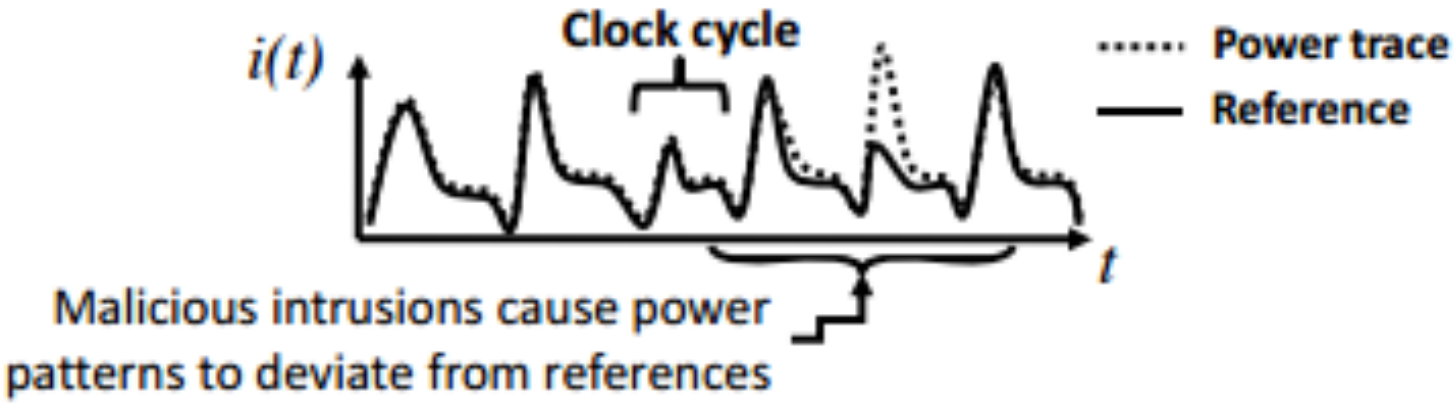
Using power consumption patterns

Power Consumption Patterns

Setup:



Power Consumption Patterns



Protection Mechanisms

- Authentication
- Access Control
- Firewall
- Intrusion Detection
- Antimalware
- Application Whitelisting
- Flow Whitelisting
- Cryptography
- Integrity Verification
- Survivability

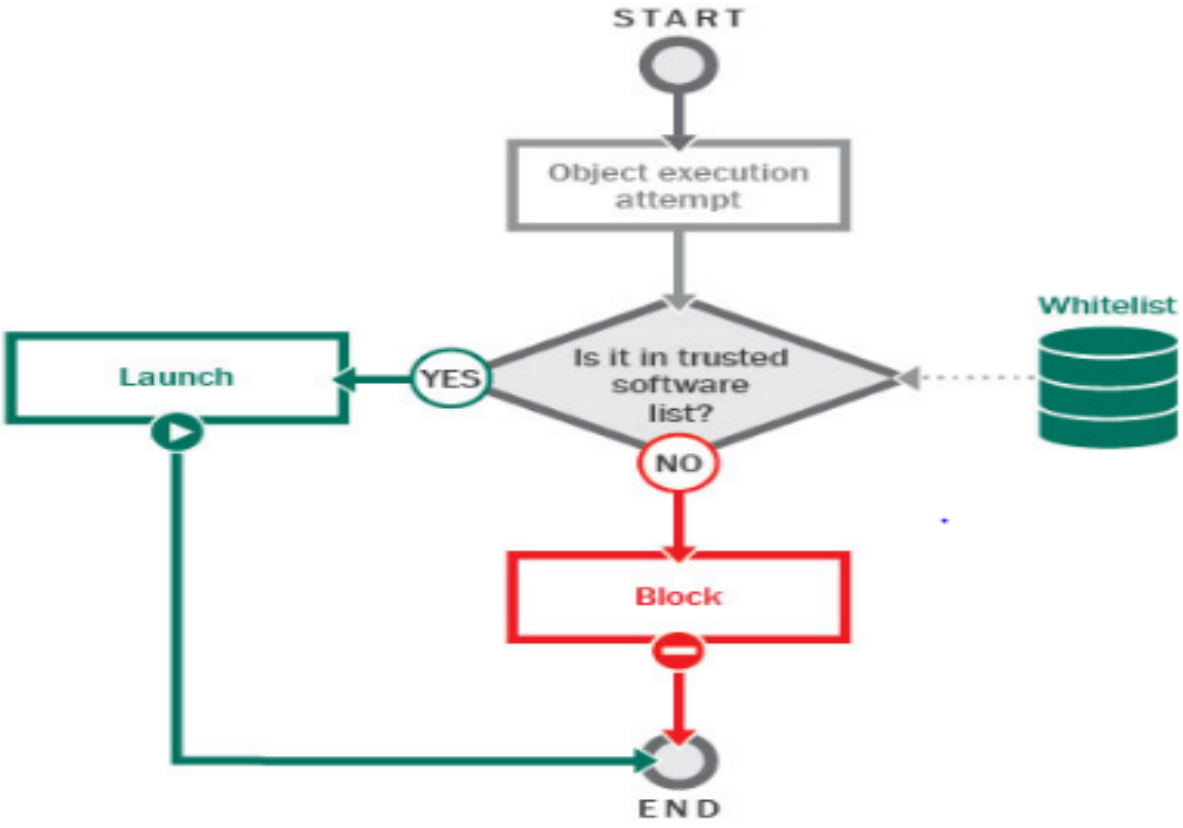
Application Whitelisting

Is the practice of specifying an index of approved software applications that are permitted to be present and active on a computer system.

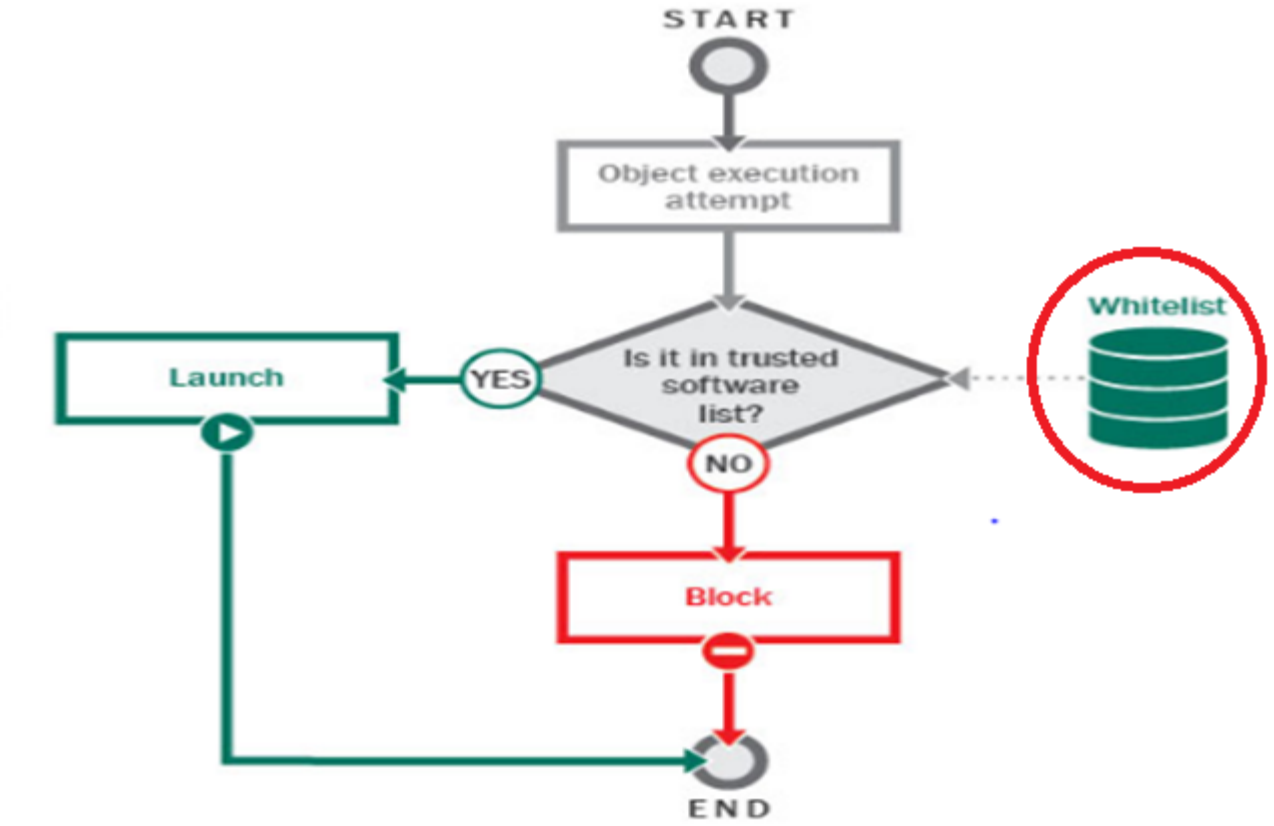
Protection Mechanisms

- Authentication
- Access Control
- Firewall
- Intrusion Detection
- Antimalware
- Application Whitelisting
- Flow Whitelisting
- Cryptography
- Integrity Verification
- Survivability

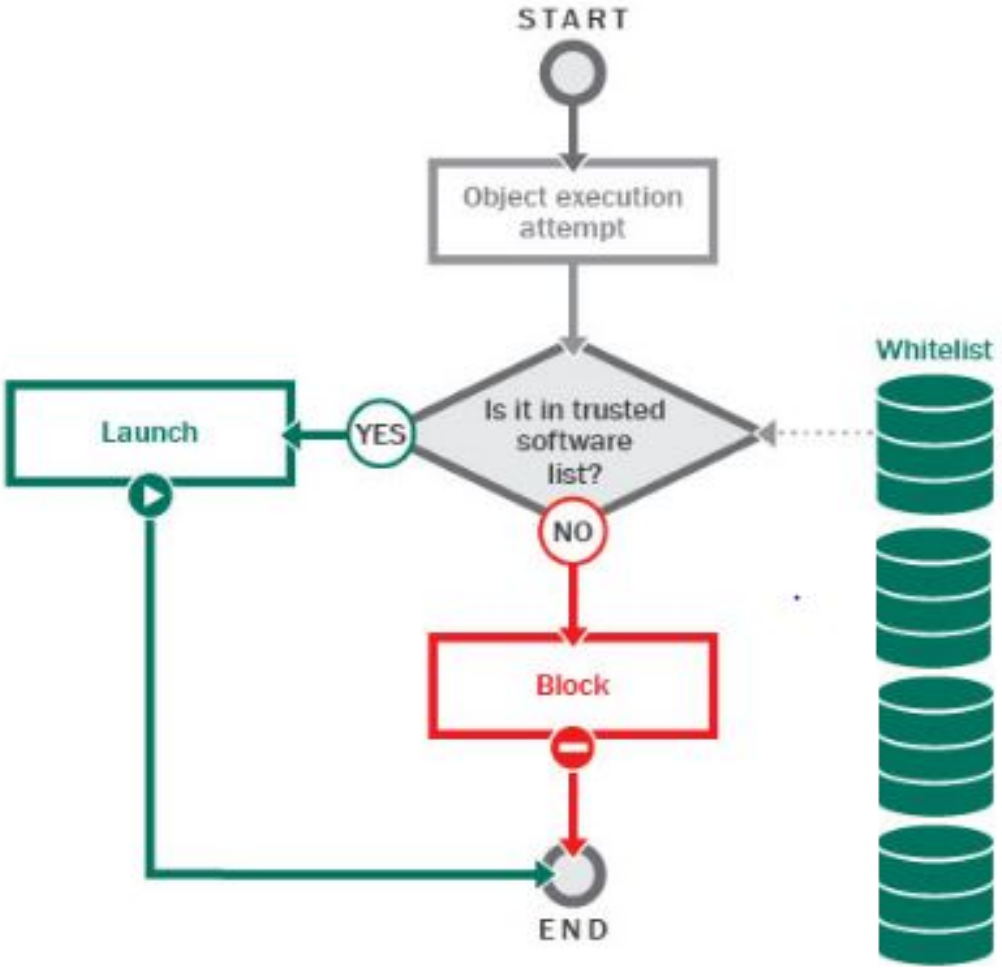
Flow Whitelisting



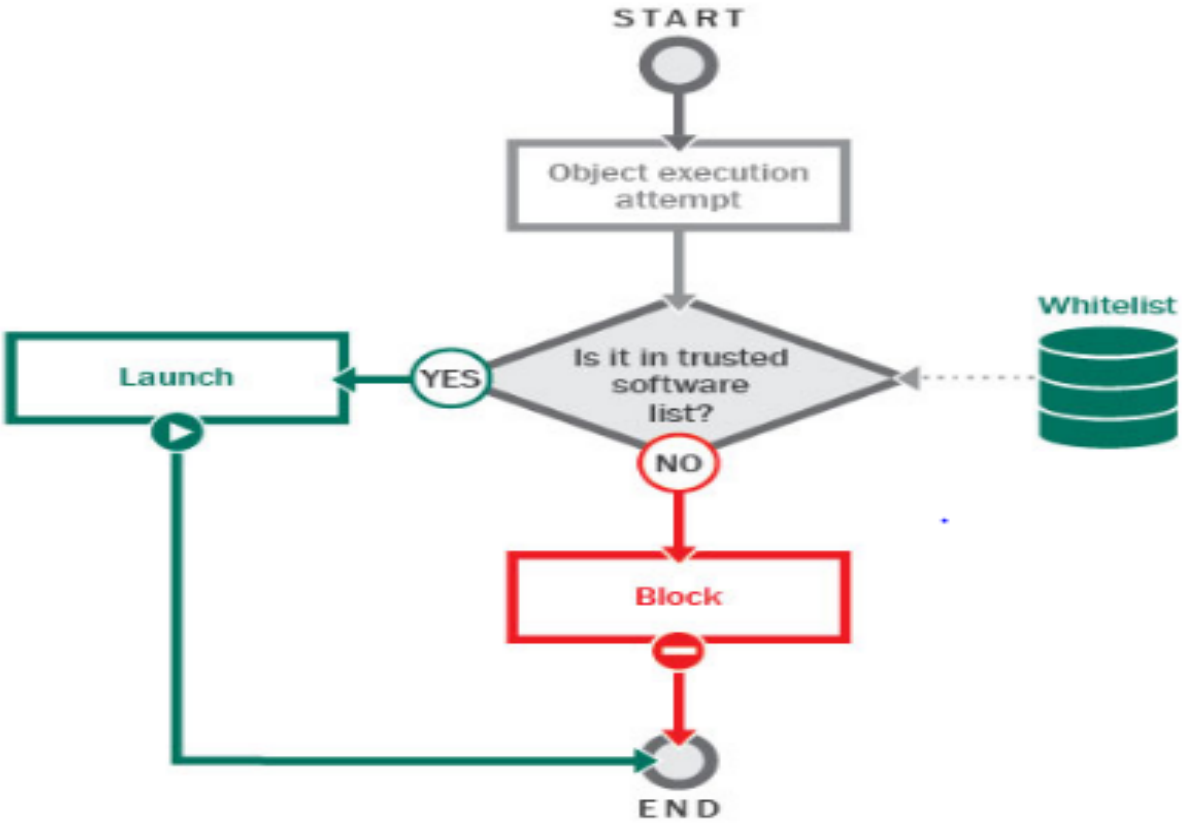
Flow Whitelisting(Main Factor)



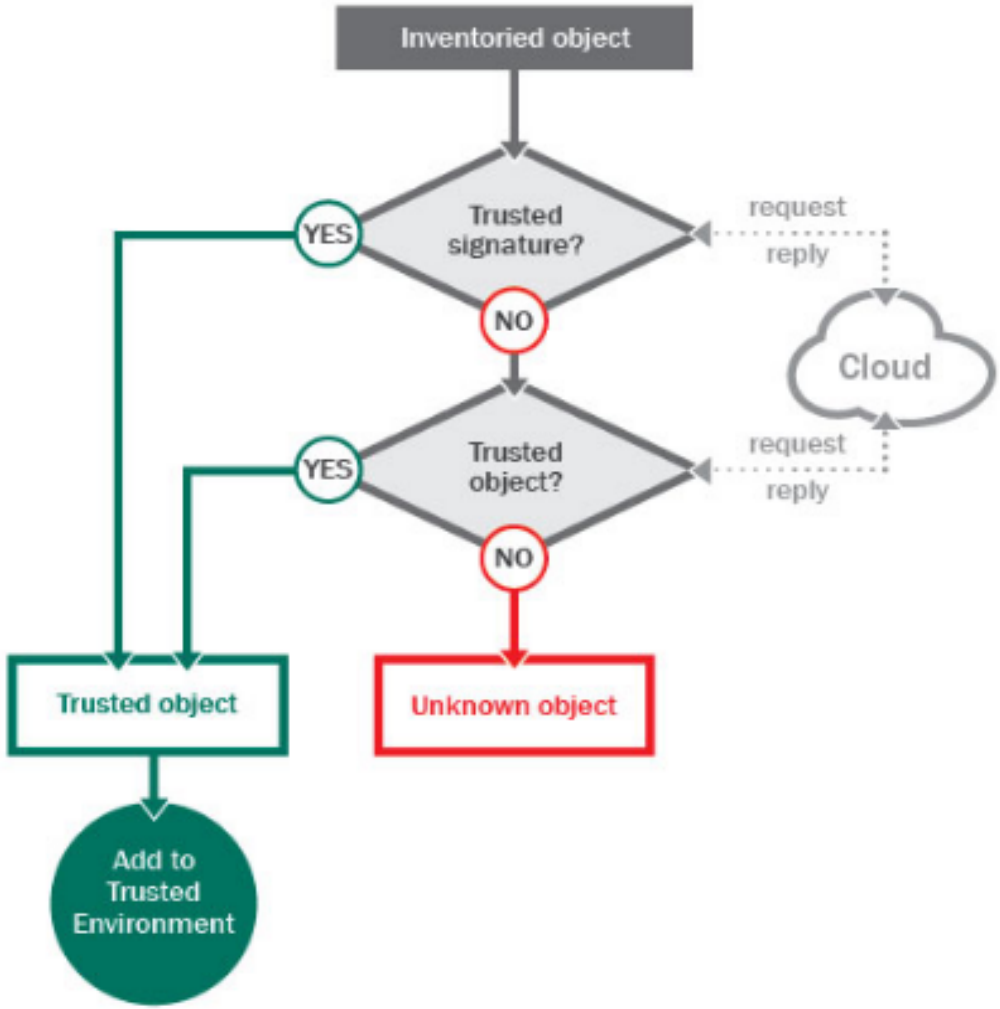
Flow Whitelisting in Internet



Flow Whitelisting in CPS



Flow Whitelisting (Learning phase)



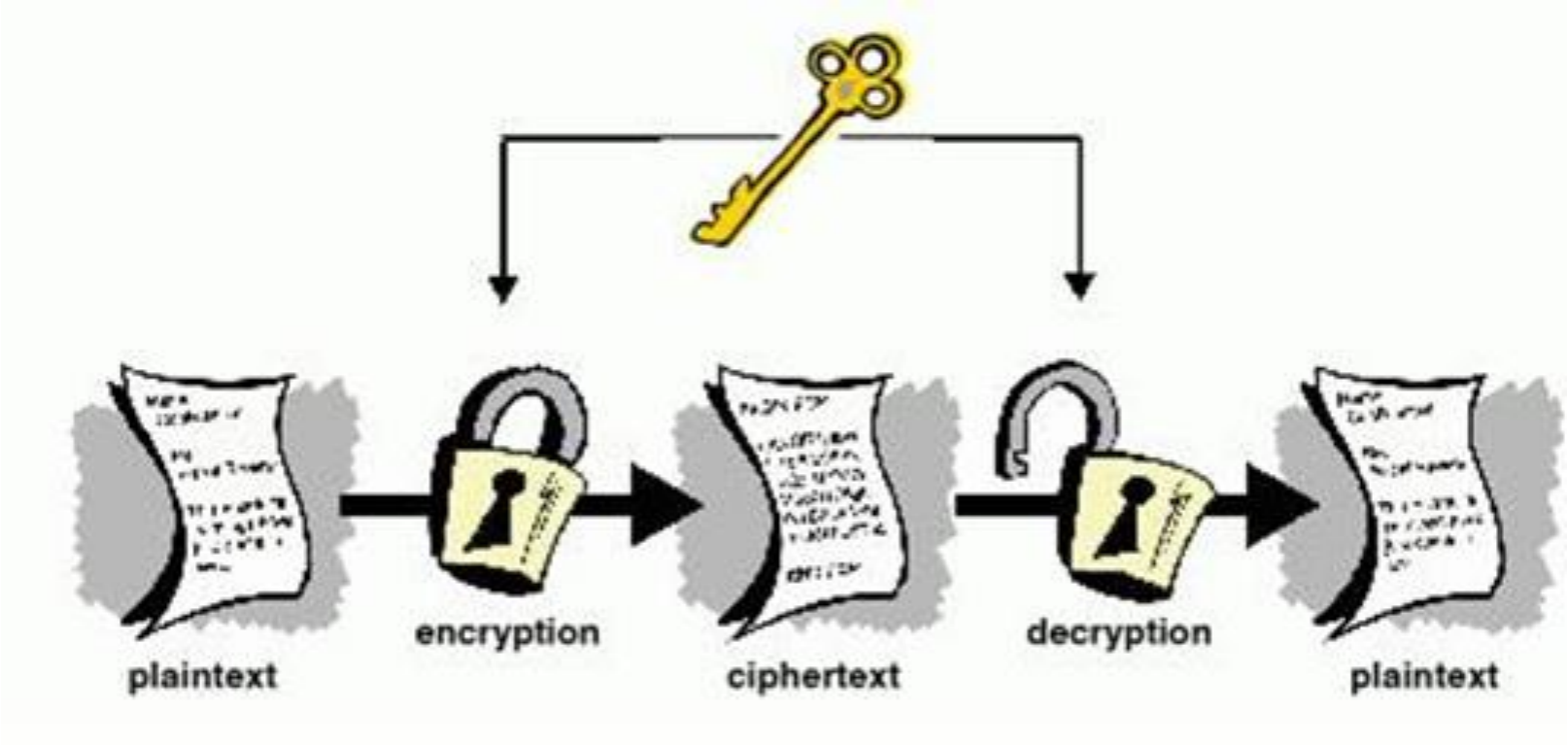
Flow Whitelisting (Learning phase)

Learning phase the network had not been under attack and all legitimate flows had been observed.

Protection Mechanisms

- Authentication
- Access Control
- Firewall
- Intrusion Detection
- Antimalware
- Application Whitelisting
- Flow Whitelisting
- Cryptography
- Integrity Verification
- Survivability

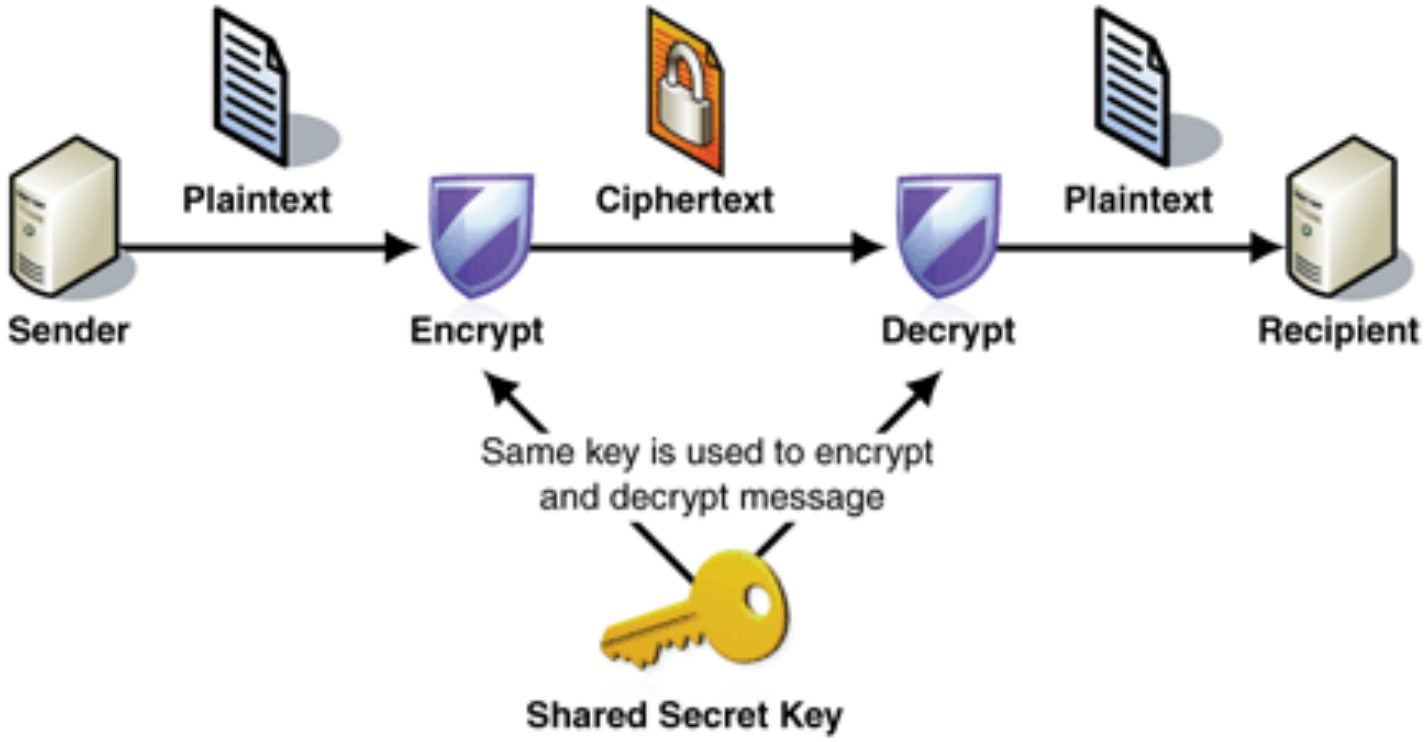
Cryptography



Cryptography

- Symmetric Ciphers
- Asymmetric Ciphers

Symmetric Ciphers



Drawback of Symmetric Ciphers

Secret key needs to be shared in a manner that cannot be intercepted by an adversary

PSKA: usable and secure key agreement scheme for body area networks.

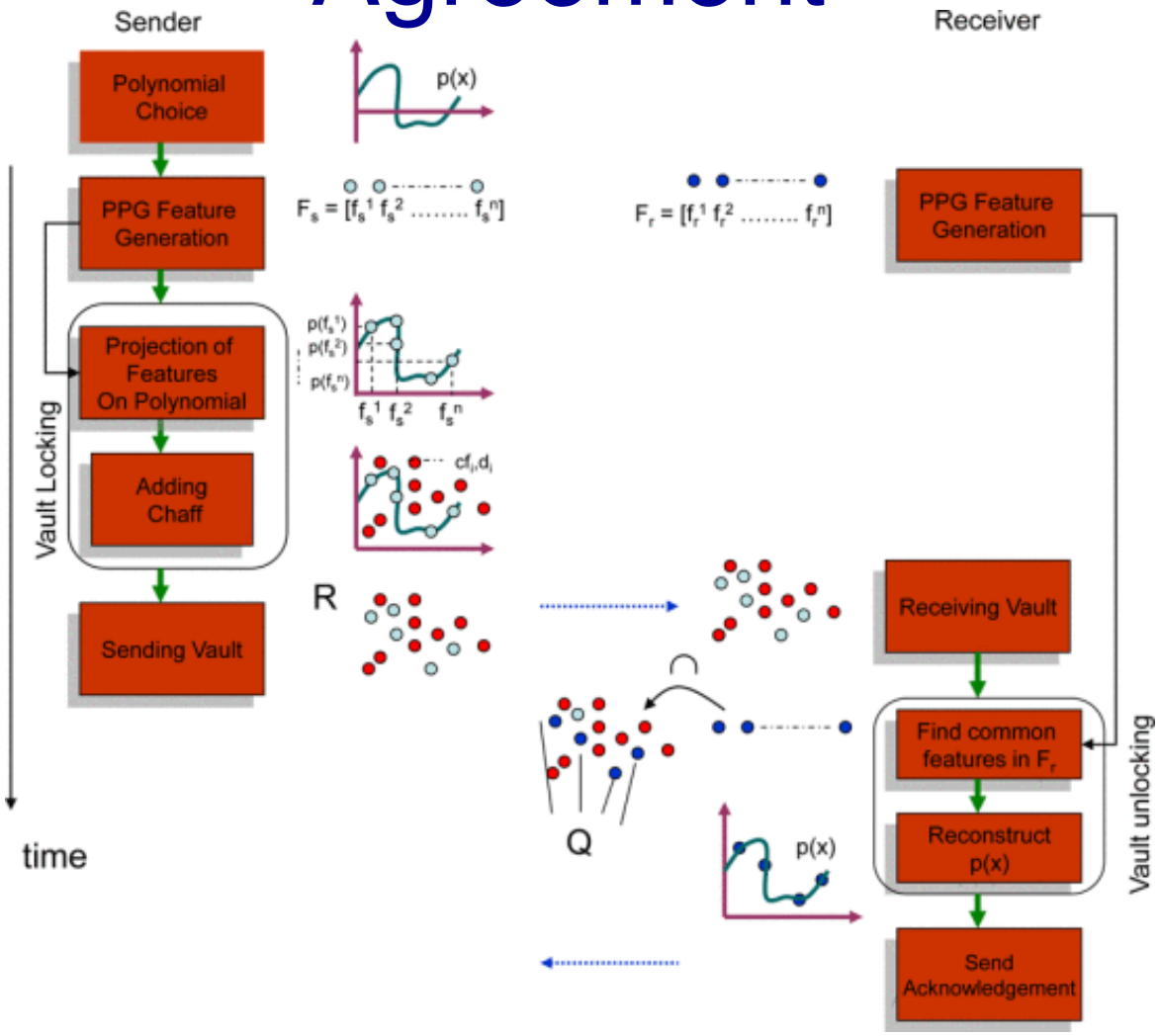
By Venkatasubramanian, K. K., Banerjee, A., and Gupta, S. K. S. (2010)

PSKA: usable and secure key agreement scheme for body area networks.

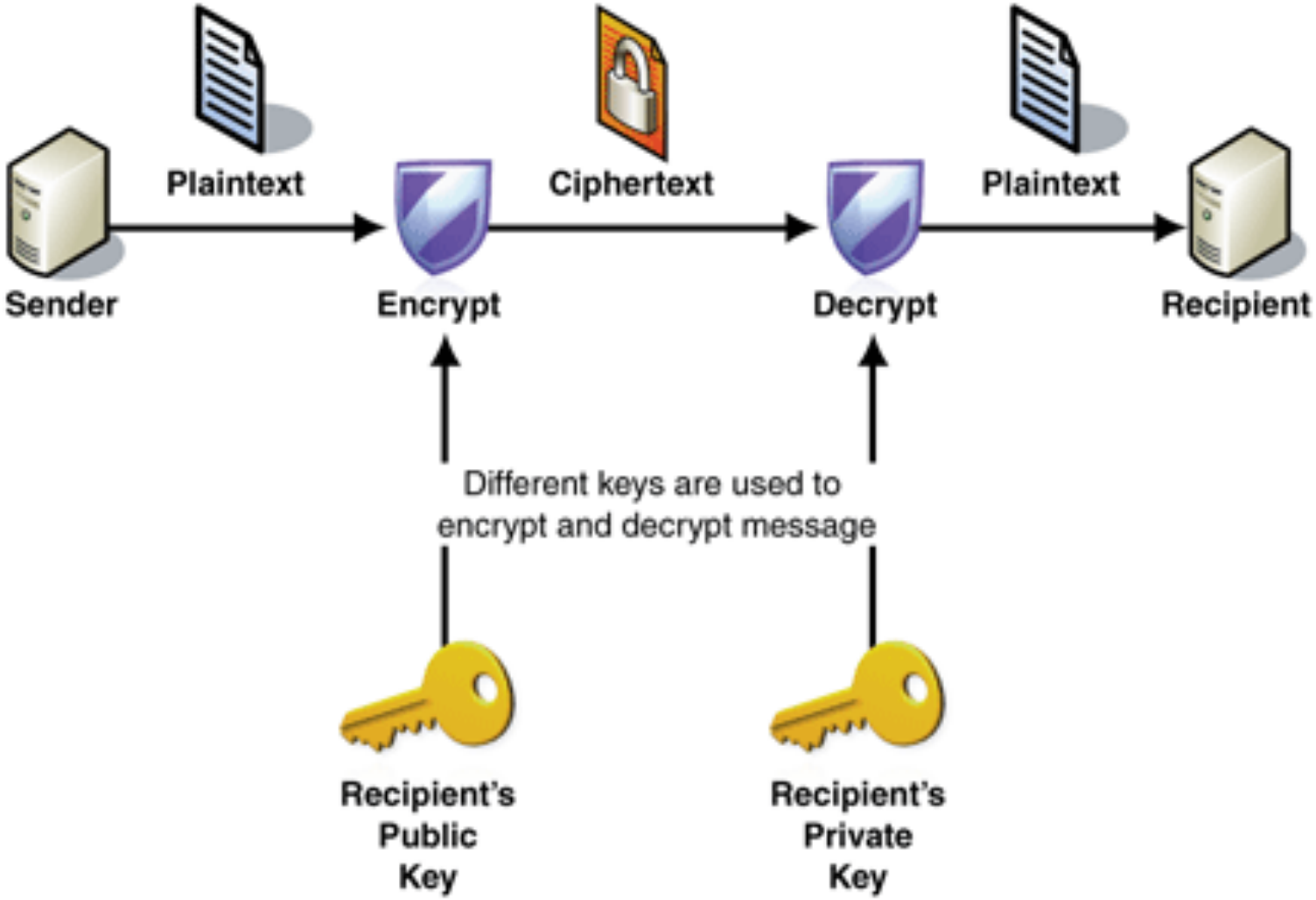
By Venkatasubramanian, K. K., Banerjee, A., and Gupta, S. K. S. (2010)

A body's physiological state changes constantly and is quite unique at a given time

Physiological-Signal-Based Key Agreement



Asymmetric Ciphers



Drawback in Asymmetric Ciphers

For large blocks of data:

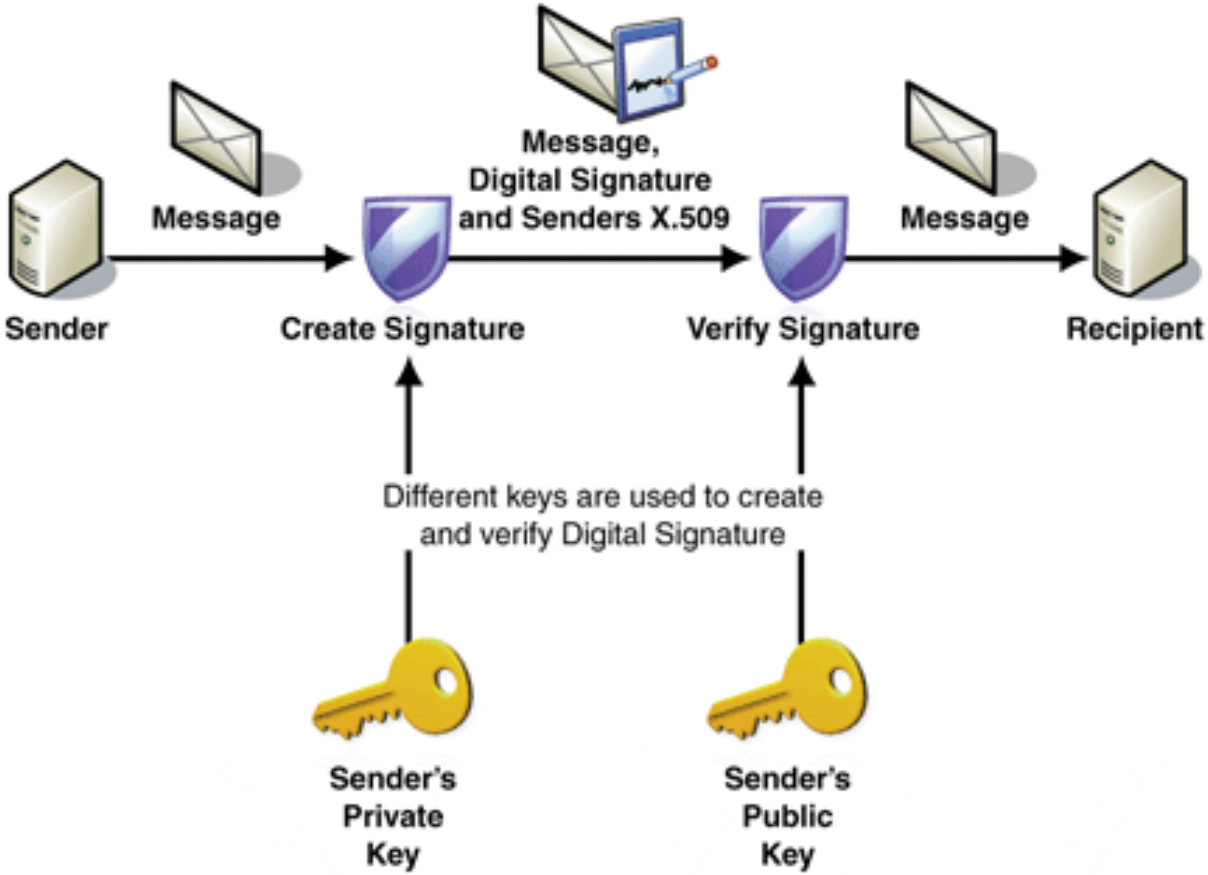
- More complicated than symmetric ones,
- Slower and
- Less practical

Symmetric cipher to encrypt the message

Asymmetric one to encrypt the secret key before sharing it with the intended recipient

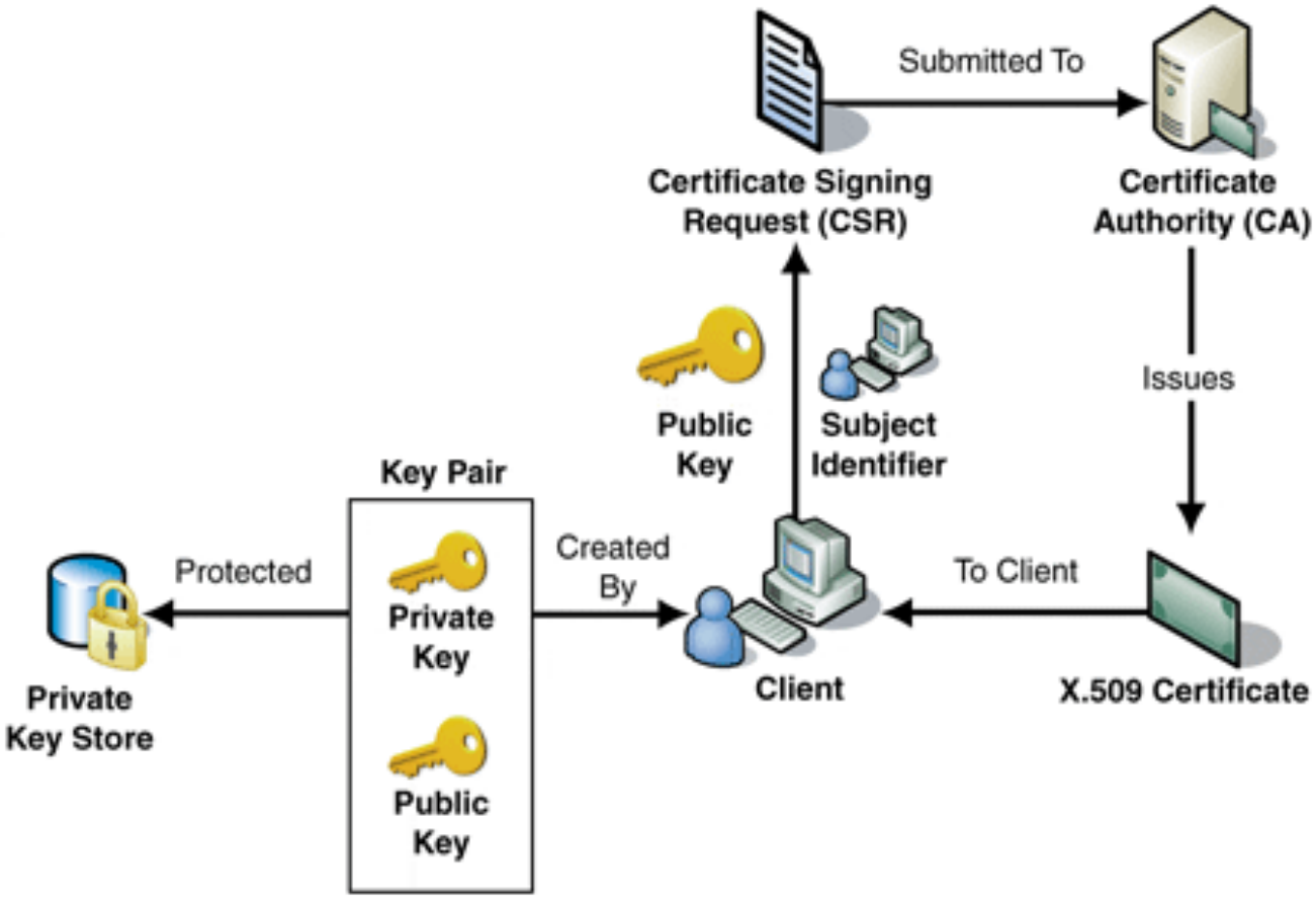
Applications of Asymmetric Ciphers

- Digital Signature:



Applications of Asymmetric Ciphers

- Digital Certificate:

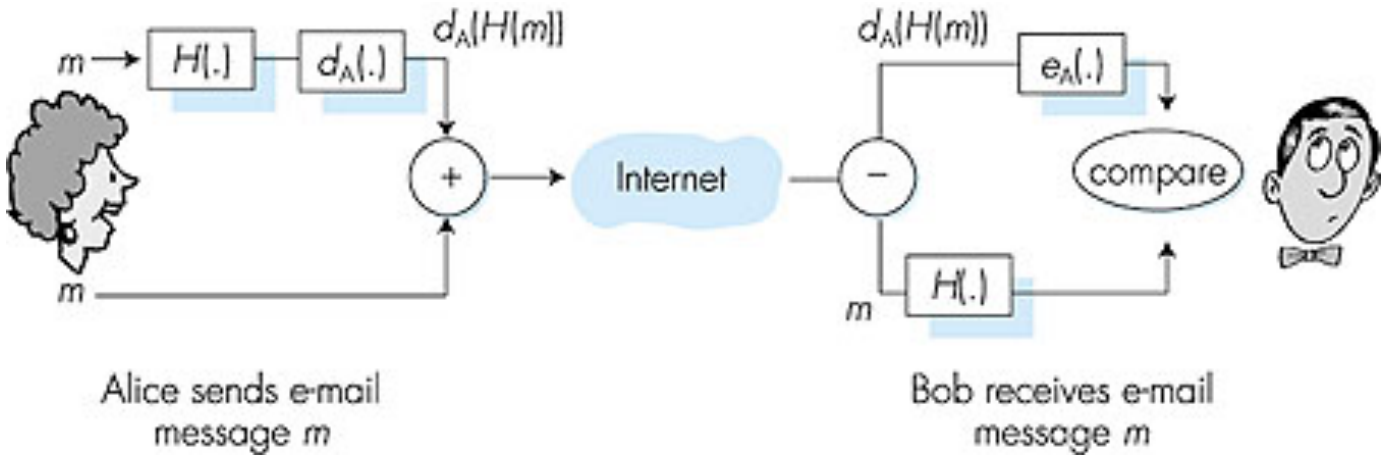


Protection Mechanisms

- Authentication
- Access Control
- Firewall
- Intrusion Detection
- Antimalware
- Application Whitelisting
- Flow Whitelisting
- Cryptography
- Integrity Verification
- Survivability

Integrity Verification

Is to compare it against a baseline file that is trusted to be correct, starting from their hashes and their sizes and continuing with more advanced tests on contents and operation.



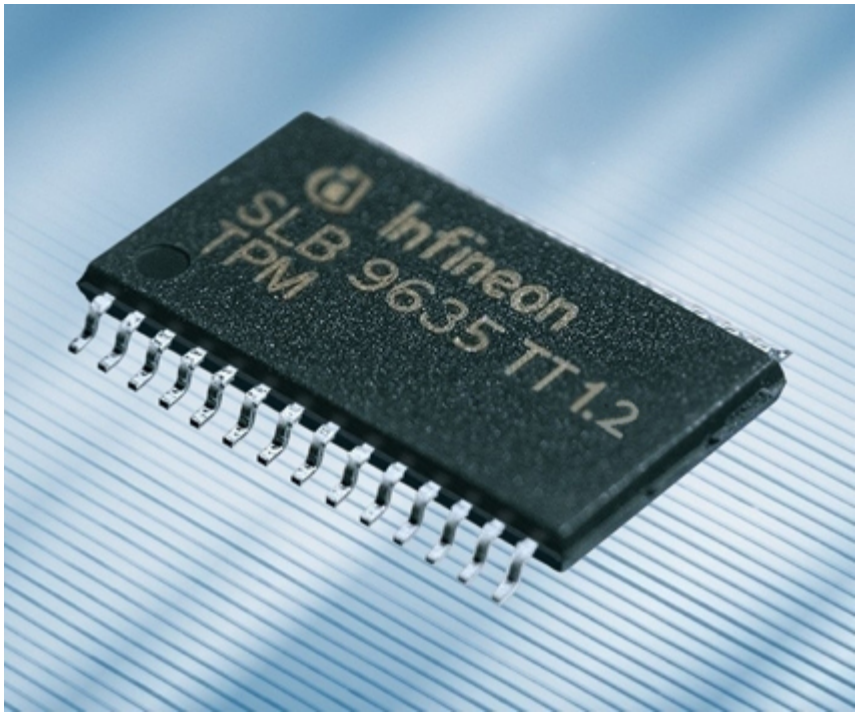
Integrity Verification(Attestation)

Process of detecting unauthorized changes on a platform (a computer, embedded system, etc.)

- Trusted Platform Module
- Software-based(challenge-response mechanism)

Trusted Platform Module

Dedicated tamper-resistant microprocessor chip



Software-based (challenge-response mechanism)

(key)

challenge

F(key, challenge)

(key)

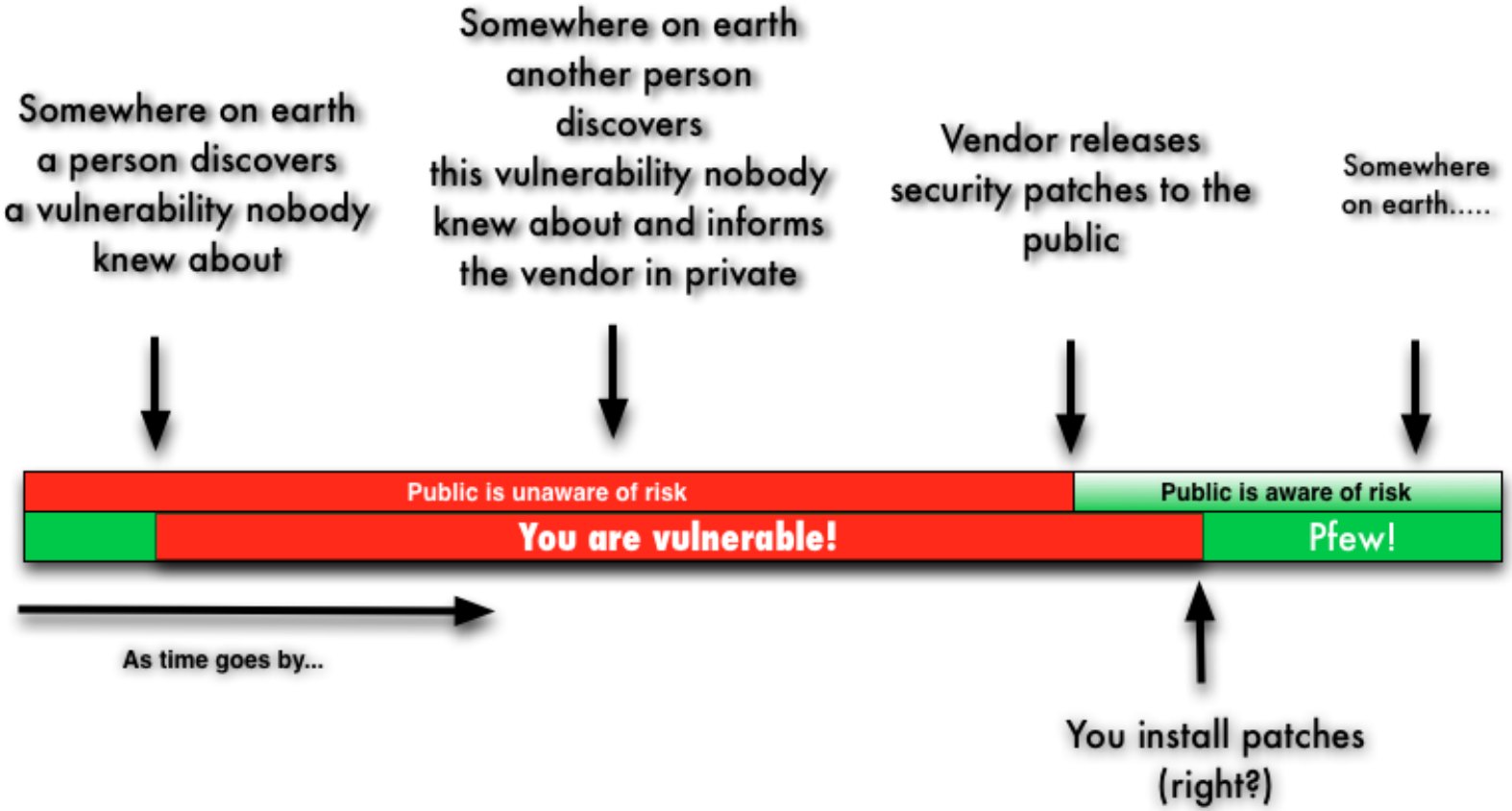
- Hardware-based attestation is reliable

- Software based attestation can be used in resource constrained embedded systems such as smart meters.

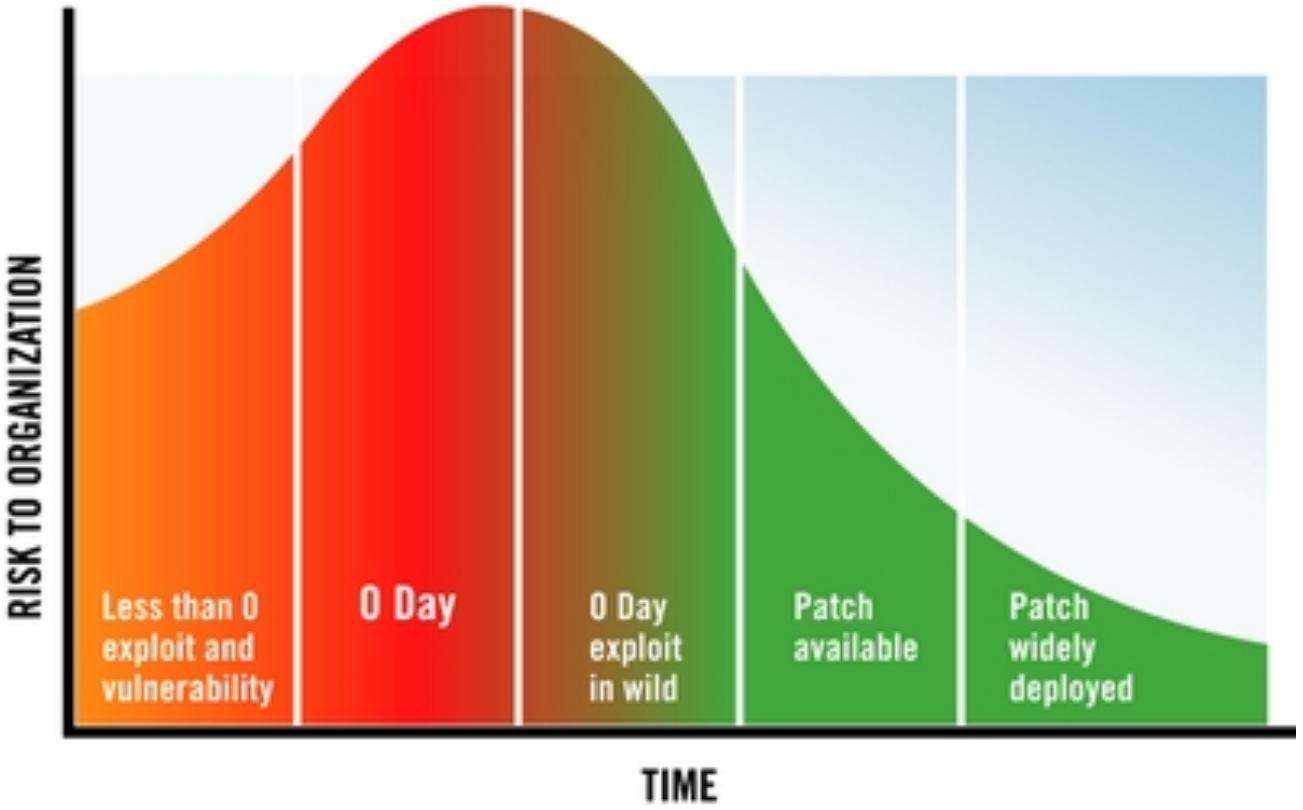
- Hardware-based attestation is reliable

- Software based attestation can be used in resource constrained embedded systems such as smart meters.

Zero-day exploits



Zero-day exploits(Risk Factor)

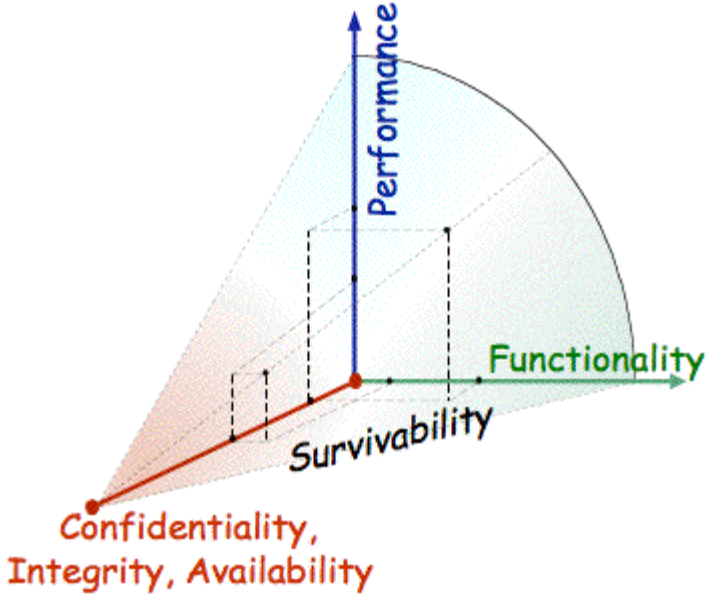


Protection Mechanisms

- Authentication
- Access Control
- Firewall
- Intrusion Detection
- Antimalware
- Application Whitelisting
- Flow Whitelisting
- Cryptography
- Integrity Verification
- Survivability

Survivability

Ability of a system to operate correctly and with minimal performance degradation even if malicious actors have compromised parts of it



Survivability

Redundancy:

- Simple redundancy
- Diversity
- Hot Standby
- Replication

Topics to be covered:

- Protection Mechanisms
- Secure Design Principles

Secure Design Principles

Based on the idea of *simplicity* and *restriction*

Simplicity

- Less to go wrong
- Fewer possible inconsistencies
- Easy to understand

Restriction

- Minimize access power
- Inhibit communication

Secure Design Principles

- Economy of Mechanism
- Defense-in-Depth
- Least-Privilege
- Separation of Privilege
- Minimization of Attack Surface
- Isolation
- Open Design
- Psychological Acceptability

Economy of Mechanism

- Keep the design and implementation as simple as possible
  - Keep It Simple, Silly! Principle

- Simpler means less can go wrong
  - And when errors occur, they are easier to understand and fix

Economy of Mechanism

- Keep the design and implementation as simple as possible
  - Keep It Simple, Silly! Principle

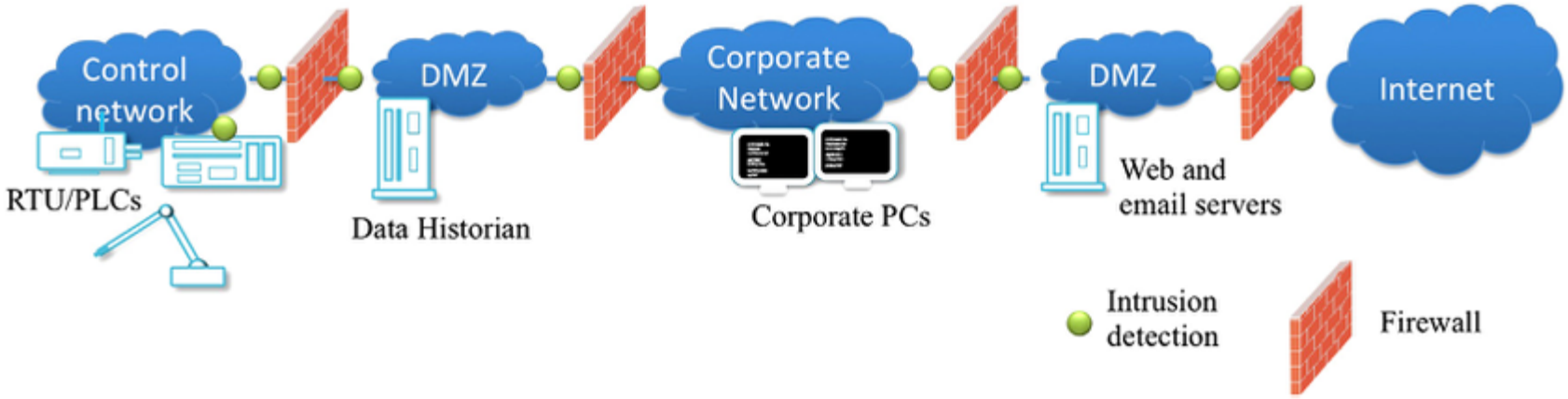
- Simpler means less can go wrong
  - And when errors occur, they are easier to understand and fix

Secure Design Principles

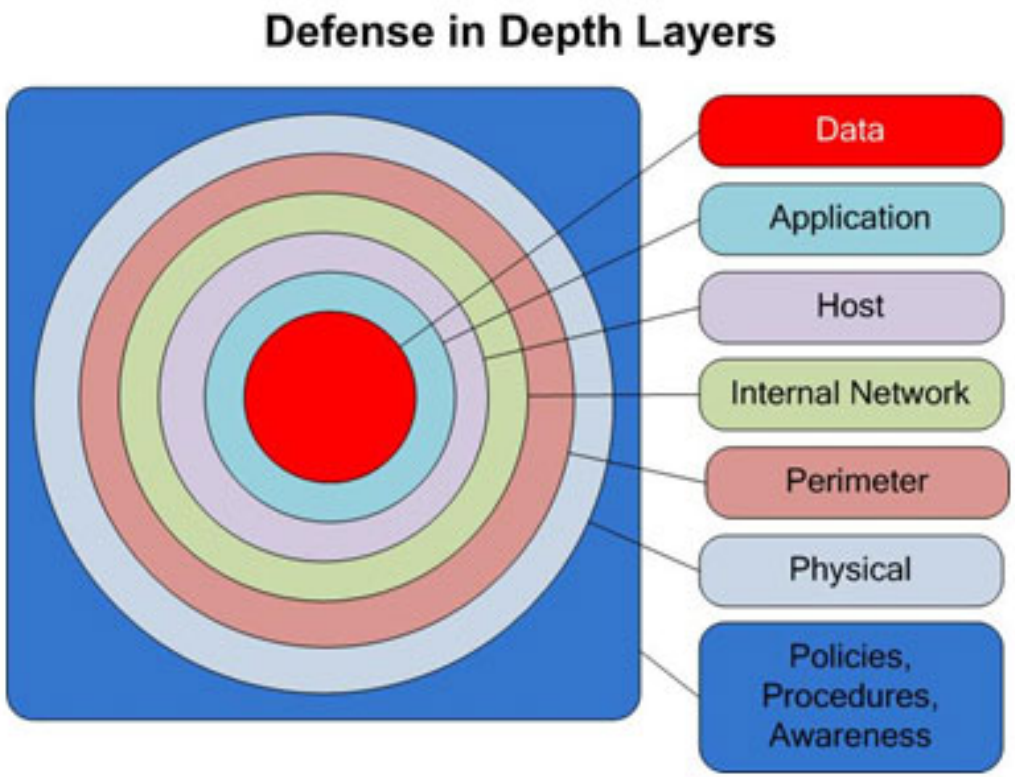
- Economy of Mechanism
- Defense-in-Depth
- Least-Privilege
- Separation of Privilege
- Minimization of Attack Surface
- Isolation
- Open Design
- Psychological Acceptability

Defense-in-Depth

Multiple levels of protection



Defense-in-Depth



Secure Design Principles

- Economy of Mechanism
- Defense-in-Depth
- Least-Privilege
- Separation of Privilege
- Minimization of Attack Surface
- Isolation
- Open Design
- Psychological Acceptability

Least-Privilege

- A subject should be given only those privileges necessary to complete its task
  - Function, not identity, controls
    - Role Bases Access Control!
  - Rights added as needed, discarded after use
    - Active sessions and dynamic separation of duty
  - Minimal protection domain
    - A subject should not have a right if the task does not need it

Secure Design Principles

- Economy of Mechanism
- Defense-in-Depth
- Least-Privilege
- Separation of Privilege
- Minimization of Attack Surface
- Isolation
- Open Design
- Psychological Acceptability

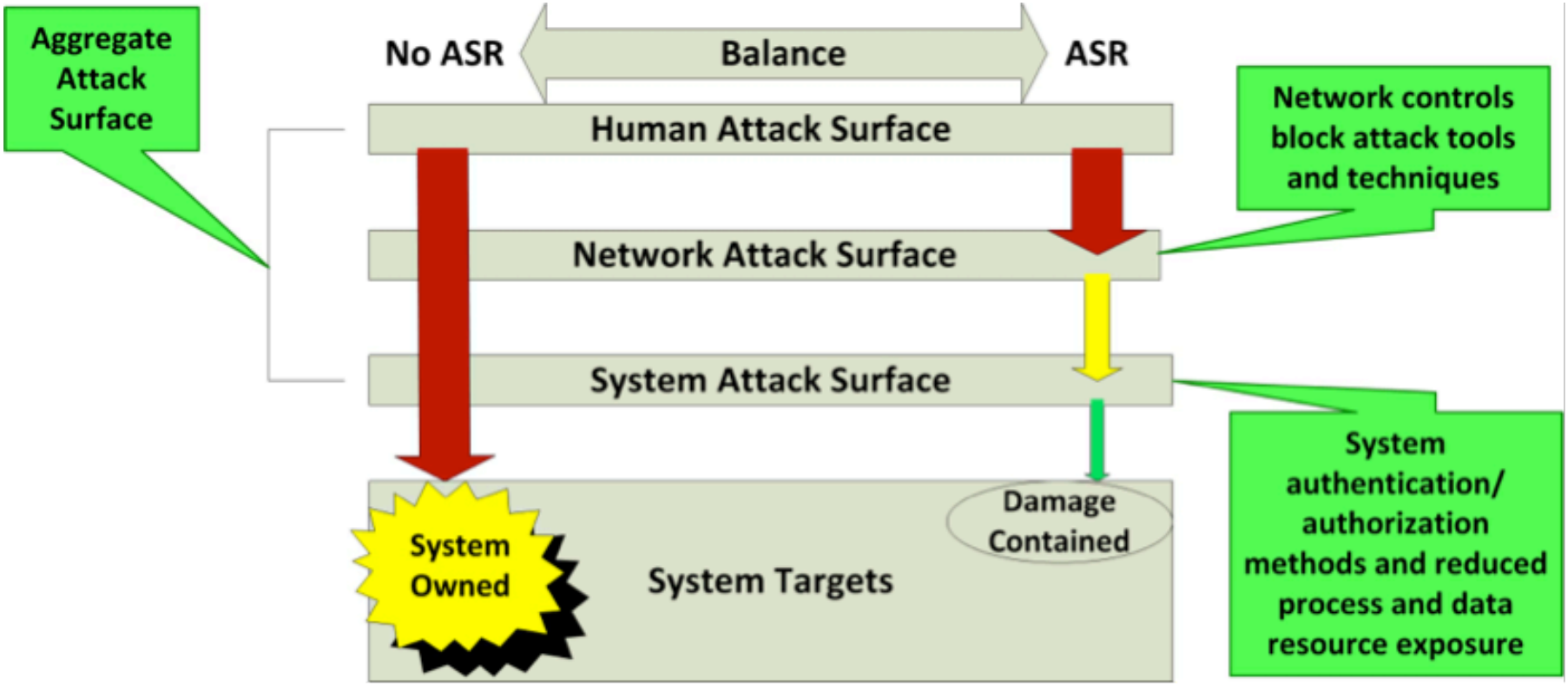
Separation of Privilege

- Require multiple conditions to grant privilege
  - Example: Checks of $70000 must be signed by two people

Secure Design Principles

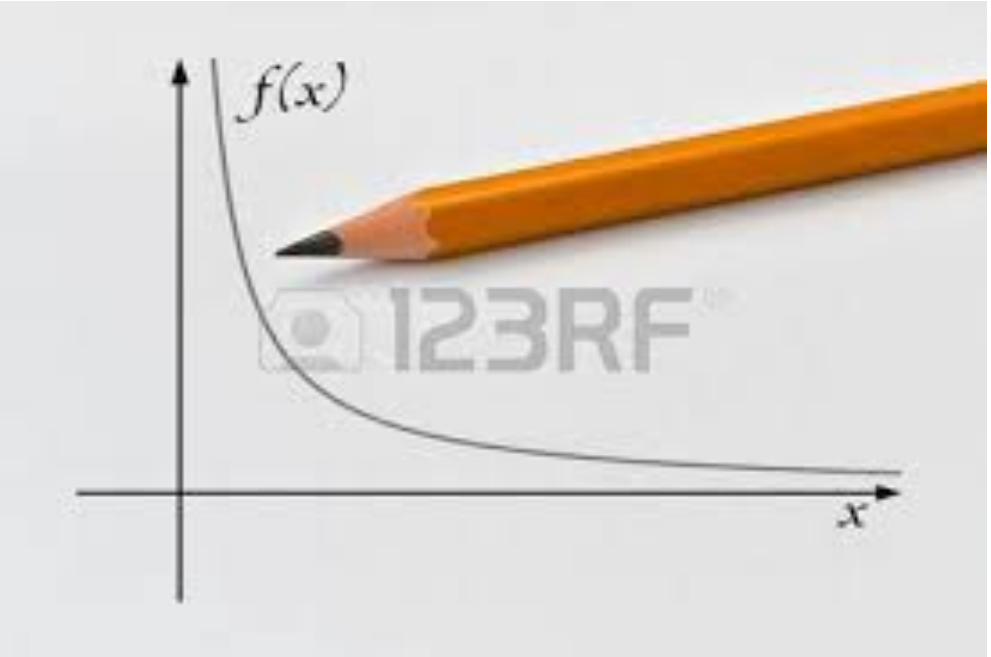
- Economy of Mechanism
- Defense-in-Depth
- Least-Privilege
- Separation of Privilege
- Minimization of Attack Surface
- Isolation
- Open Design
- Psychological Acceptability

Minimization of Attack Surface



Minimization of Attack Surface

Minimization of the attack surface is in direct contrast to the increasing functionality of modern cyber-physical systems

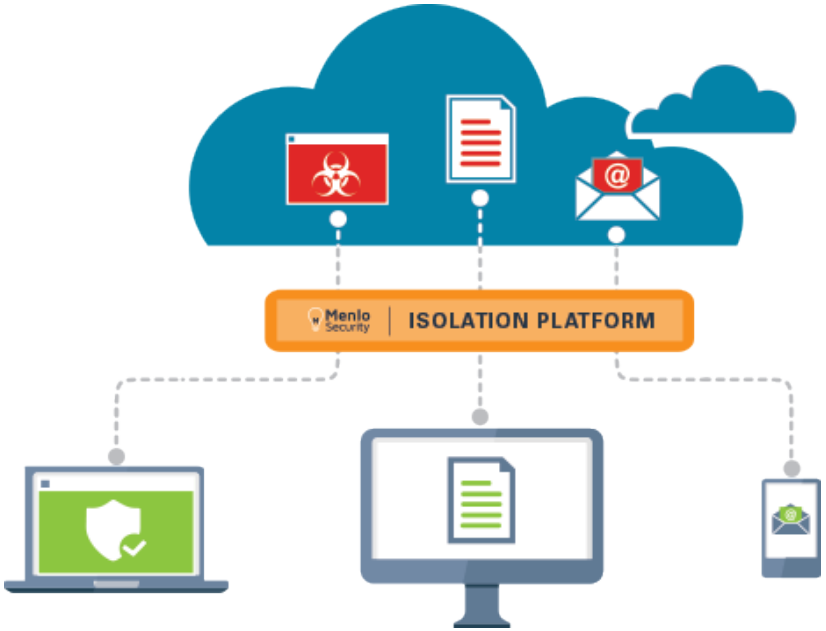


Secure Design Principles

- Economy of Mechanism
- Defense-in-Depth
- Least-Privilege
- Separation of Privilege
- Minimization of Attack Surface
- Isolation
- Open Design
- Psychological Acceptability

Isolation

Isolate subsystems from each other, a user's processes, and data from other users', and critical resources from external or public access.



Secure Design Principles

- Economy of Mechanism
- Defense-in-Depth
- Least-Privilege
- Separation of Privilege
- Minimization of Attack Surface
- Isolation
- Open Design
- Psychological Acceptability

Open Design

- Security should not depend on secrecy of design or implementation
  - **Popularly misunderstood to mean that source code should be public
  - **Does not apply to information such as passwords or cryptographic keys

Secure Design Principles

- Economy of Mechanism
- Defense-in-Depth
- Least-Privilege
- Separation of Privilege
- Minimization of Attack Surface
- Isolation
- Open Design
- Psychological Acceptability

Psychological Acceptability

- Security mechanisms should not add to difficulty of accessing resource
  - Hide complexity introduced by security mechanisms
  - Ease of installation, configuration, use
  - Human factors critical here