IS YOUR LIVE VIDEO AND DATA SAFE?

From both external and insider threats?

ABSTRACT

Video and data within a physically secure environment, such as a command-and-control center, an isolated production suite, a network operations center (NOC), a broadcast control room, and even within a super locked-down, Sensitive Compartmented Information Facility (SCIF), is considered safe and secure. But is it?

Learn how to determine if your system is secure or not and discover some surprising facts.

Howard Sutton, P.Eng MBA CFA

[April 2021]

Is Your Live Video And Data Safe?

In the current cybersecurity environment, live video and data distributed within physically secure environments, such as a Sensitive Compartmented Information Facility (SCIF) or briefing centers, is no longer safe and secure. SCIFs and other traditional command and control systems have historically used matrix routers with uncompressed baseband signals such as SDI or HDMI, and control signals such as KVM However, these video distribution systems were architected decades ago without information security as a priority. Uncompressed baseband signals were designed for easy connectivity and reliable viewing of low latency, high-resolution video. The benefits of accessibility come at the steep cost of glaring security vulnerabilities.

The baseband standards that guarantee compatibility between devices allow anyone to connect a cable and immediately view, hear, or record any of the signals. For missions where data and video confidentiality are paramount to success, the vulnerabilities presented by uncompressed baseband signals are unacceptable.

Matrix Routers – Not Designed For Security

Matrix routing environments are vulnerable to intentional and accidental exposure of data. A matrix router, also known as a video matrix switch, has been pervasive in broadcast and other video intensive applications, including command and control (C2) environments for routing multiple input sources (cameras, computers, satellite receivers, and certain audio/video sensors) to one or more destinations (displays, information walls, computers). Because any source can be routed to any destination, the internal function is driven by crosspoints. When activated, the crosspoint chip passes the input port content to the desired output port.

The design includes guaranteed bandwidth and a non-blocking architecture. Routers are configured using routing tables that define which specific input port can connect to which defined output port. The router can connect baseband signal flows between transmitter ports on the input half of the router and receiver ports on the other half of the router only if a deliberate, logical connection is established. The security policy for baseband routers is based on these connections. The only method to create groups with a matrix router is by its controller; however, the root baseband signal is exposed within the router matrix. Segmentation for Multiple Independents Levels of Security (MILS) is implemented in the baseband matrix router through this method.

The benefit of any matrix switch using routing tables with appropriate configuration software is an open connection without restrictions, but it is also a cybersecurity weakness. While the signals are received and transferred through the router, they are not encrypted. Each and every port has viewable video. Any input port can be connected to any output port and allow someone to instantly view, hear, or capture confidential content. The router relies on its control system to provide security to protect the video. Each destination device attached to the router is viewable. Every destination is vulnerable. An example of a significant security shortcoming is that when a device is unplugged at the destination, the video continues to flow from the router. A recording device could be attached, and the router will continue to send classified video to malicious actors. Physical security is required throughout the enterprise. There is no authentication in baseband routers other than what is defined in the configuration table for each port.

Matrix routers were never designed for security or networking. The inability to encrypt uncompressed baseband signals is an insurmountable hurdle to overcome for matrix routers. All baseband routers have failed Defense Information Systems Agency (DISA), Joint Interoperability Test Command (JITC) certifications from 2019 onward as none have FIPS 140-2 encryption.

Insider Threats

Insider threats are a rapidly growing concern in cybersecurity, and interest in countering these threats through encryption is growing as a result. The Verizon Data Breach Investigations Report 2020 (DBIR), which examined nearly 4,000 security breaches, discovered 30% of cyber security incidents involved internal actors within a company.

Research shows that data encryption from end-to-end is the most effective cybersecurity countermeasure to both internal and external actor threats. Matrix routers signals cannot use secure transport protection in either the essence (video/audio) nor the control. Furthermore, due to the lack of encryption, matrix routers cannot use keys, tokens, or certificates. If the data is not encrypted, anyone can plug in an extender to any port on the matrix router and view the content. In today's threat accentuated environment, video distribution solutions must do their part to protect against both insider and external threats. Baseband data cannot be secured with encryption, and so matrix routers are not secure for sensitive video or data due to their open, unencrypted, and easily accessible structure. Matrix routers are not a secure option when security is critical.

Security Certifications Revealed

Even matrix router systems that claim security certifications are susceptible to the same vulnerabilities. Security certifications vary based on what each certification entails and what specifically is tested. Certifications also vary widely in stringency, with some certifications that demand achieving specific technical capabilities and some certifications that allow for vendors to self-author their own arbitrary security targets and evaluate themselves to determine if they

Certifications

Environments determine the correct and most valuable certifications. Some of these certifications are **FIPS, DoDIN APL, Common Criteria (CC)** and **CSfC**

FIPS: Federal Information Processing Standard (FIPS)" was developed by the U.S. **National Institute of Standards and Technologies (NIST)** in 1994 for validation of the use of cryptography in security systems. FIPS has several levels:

Level 1: Cryptographic
Level 2: Tamper Evidence
Level 3: Physical Tamper resistance
Level 4: Environmental+ Zeroization

Software applications are Level 1.

Advanced Encryption Standard (AES 256/128) is required for FIPS 140-2 Encryption is mandated by DoDIN that ALL IP use FIPS 140-2/3 certified modules.

FIPS equals Cryptography. It is **NOT…**

- Certificates
- Public Keys
- Tokens
- Others

Key management - Suite B Cryptography

- Advanced Encryption Standard (AES) with key sizes of 128 and 256 bits.
- Elliptic Curve Digital Signature Algorithm (ECDSA)
- Elliptic Curve Diffie–Hellman (ECDH) – key agreement
- Secure Hash Algorithm 2 (SHA-256 and SHA-384) – message digest

DoDIN APL. The Defense Information Systems Agency (**DISA**) manages testing of products to be placed on the Department of Defense Information Network (**DoDIN**) Approved Products List (**APL**). The APL is the single consolidated list of products that have completed **Interoperability (IO)** and

meet their own requirements

The Evaluation Assurance Level (EAL) is a defined testing process, which defines the thoroughness of the testing procedure and each EAL has a security target. However, the protection that these certifications provide can be very misleading as the security target can be self-defined by the product's vendor. This is like a fox defining the security requirements of a hen house. It could also be considered a doorknob certification. For example, if the security target is defined as a doorknob that turns to the right to open the door and then the test confirms it opens the door, it passes certification. The doorknob does not add to security, it does not lock against intruders nor does it prevent unauthorized personnel from turning it. It is not even required for security. However, under the EAL conditions, if it performs as stated by simply turning and opening the door with no security benefits, it passes EAL certification.

National Information Assurance Partnership (NIAP) Protection Profiles (PP) on the other hand are well defined and articulated targets that are consistent across products. North America tightened up Common Criteria (CC) with PPs, whereas some other countries, such as Norway, are still performing CC with EALs. This accepted practice of inconsistent standards is why it is important for a perceptive customer to thoroughly scrutinize the security targets to understand the scope and limitations of what is genuinely being tested.

Often these targets explicitly state that the system under test must include both physical security in a closed environment for the entire system and have trusted users in order for them to be secure. The combination of physical security and trusted users is unfortunately blind to the severe risk of insider leaking, whether deliberate or accidental, which many experts consider a naive oversight at best and deliberately misleading at worst. An analogy to this concept is driving an armored truck filled with cash through the city with its back doors wide open, yet the company states the money in the truck is secure since all of the citizens in the city are trusted. All the bulletproof glass, steel plate pillars, and Kevlar bolstered doors that secure that armored truck are now rendered utterly useless by the open back door. The trouble is people cannot be trusted. These are the insider threats. People can be nefarious, and they can also make mistakes, leading to leaked data.

Certifications Continued

Cybersecurity (CS) certification. Joint Interoperability Test Command (**JITC**) is an approved testing center for **IO** and **CS** certification.

Common Criteria (CC) is focused on other areas of IT project security functions. It consists of **Evaluation Assurance Level (EAL)** tests to assure conformance to a security target.

- Level 1: Functionality Tested
- Level 2; Structurally Tested
- Level 3: Methodically Tested
- Level 4: Methodically Designed and Tested
- Level 5: Semi-Formally Designed and Tested
- Level 6: Semi-Formally Verified Design and Tested
- Level 7: Formally Verified Design and Tested

A higher level does not mean a harder test. Many **EAL** security targets are written by the vendors themselves and amount to no more than a "Doorknob certification", which means that they describe what it will do and then prove it does it. For instance, with a doorknob you would grab the handle and turn either right or left and the door should open. If it opens, then the doorknob passes. The most important part to look at with an EAL certification is the **security target**. Read and understand what it says. Does it contain a protection profile?

Protection Profile (**PP**) is a document used as part of the certification process according to ISO/IEC 15408 and the Common Criteria (CC). As the generic form of a Security Target (ST), it is typically created by a user or user community and provides an implementation independent specification of information assurance security requirements. A **PP** is a combination of threats, security objectives, assumptions, security functional requirements (**SFR**s), security assurance requirements (**SAR**s) and rationales.

Tempest, which is a pre-IP network artifact, was concerned with spies exploiting the electromagnetic signals and snooping for information on RF devices. Today, fiber optic IP networks are not emitting RF signals. However, the threat of easily penetrating a matrix routing environment by simply plugging in a video cable for unlimited access to sensitive data is frighteningly real. Tempest and other certifications are meaningless without a Security Target that upholds integrity to protect assets from both internal and external threats without requiring the trust of all users. Electronic snooping equipment is likely much less an immediate concern than is an insider threat with the ability to plug in an extender to any port on the matrix router and view the classified content.

IP Gateway Vulnerabilities

Some matrix router companies have attempted to bridge the security vulnerability chasm in their products by placing IP gateways to travel between an uncompressed baseband signal into an IP network. While this cobbled composite solution may be effective in scenarios where data and video confidentiality, integrity, and availability are not a high priority, the lack of end-to-end encryption and easy exposure to both internal and external threats make this attempted solution unworkable in mission critical scenarios. There are enormous vulnerabilities, inefficiencies, costs, latency issues, along with the end-to-end management and control issues. Matrix based companies will sometimes use a FIPS 140-2 encryption module only in a conversion gateway that places baseband signals onto an IP network. However, for DoDIN requirements, everything must be FIPS 140-2 compliant, and no exposed video or control information can exist anywhere on the network.

Video which is only encrypted at a gateway is still exposed and vulnerable if the end-to-end transmission is not secure. A matrix installation is not secure by only implementing an encrypted signal across the IP network portion. From a signal security perspective, matrix router based systems present a significant risk.

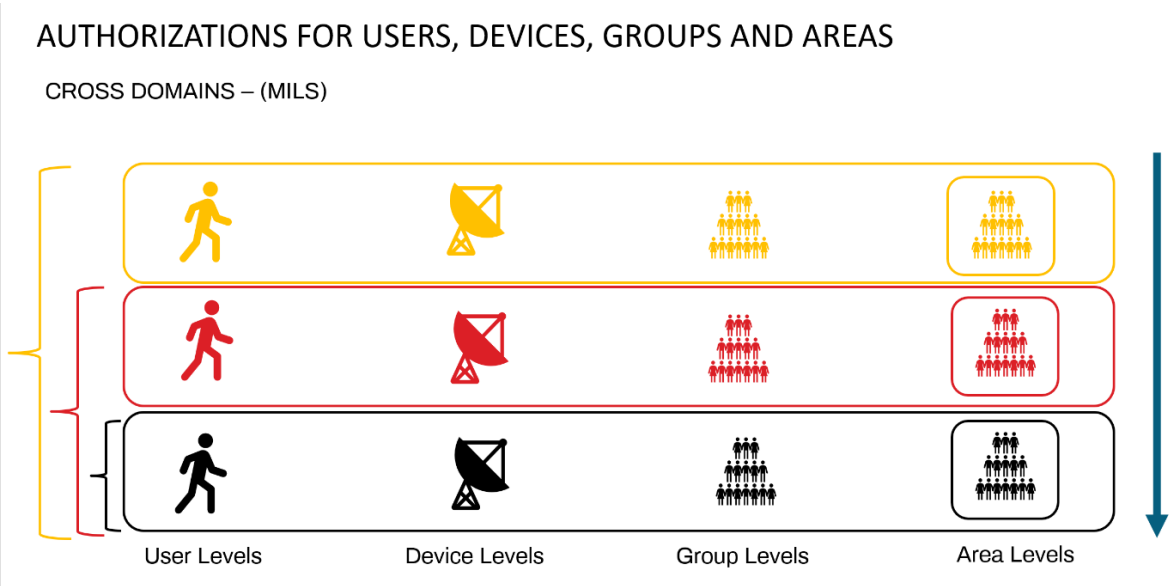
The alternative solution falls to Ethernet IP primarily because encryption is a viable option for the IP matrix. In addition to all the inherent benefits of IP architectures, including, but not limited to, distributed scalability, cost, and pervasiveness, IP Video Distribution capabilities can now provide absolute security against both internal and external

threats, while delivering, if architected properly, zero latency and ultra-high definition (4K) solutions.

Not All IP Security Is The Same

But not all IP Security is the same. Security must be designed from the ground up within the application to be truly secure. Putting a steel door on a cardboard house does not make it secure. The entire house must be built of steel to be secure. The use of certified encryption, along with advanced use of keys, tokens, and certificates completes a solution that can provide security from source to glass in a Multiple Independent Levels of Security (MILS) environment. The investments in IP and the use of IP globally over the past decades overshadows the modest use and investment in baseband. The innovation in video IP has made it possible to implement secure, reliable, MILS classifications, distributed video solutions. The advances in price/performance in combination with current programming techniques and cloud capabilities will see IP systems replace matrix video when security matters. Not in the future, but now.

The pervasiveness of IP technology in society to perform basic functions in medicine, finance, military, commercial, and others gave birth to state and non-state actors efforts to steal information and take down networks. The massive investment, billions of dollars, in making IP secure started in the 1980's. While breaches continue to be exposed, it is not because of weakness in technology, but due to the breakdown in the proper implementation in securing the technology. Actors with malicious intent are always looking for vulnerabilities. Using current capabilities and processes absolutely makes IP MILS Security superior to Baseband Multiclass security.



The objective of the IP video transmission is to ensure the user, confirmed by the seat assignment and authentication, securely receives, and transmits data, according to the assigned MILS level and only the intended information. Delivering a secure platform for MILS secure IP requires the product to be designed from the ground up with this objective. Without an appropriate architecture, supported by a clearly articulated and well-defined process, the solution is vulnerable. Taking legacy applications and metaphorically sprinkling security dust on

top does not patch the gaping security holes in security. There are a variety of ingredients that must be properly designed to implement a secure IP MILS classification, multi-domain enabled distributed network.

Security is not generic, details do matter. Companies claiming IP security and cybersecurity is a normal practice, independent of the degree or level of security. Buyers must be aware and know the questions to ask in order to determine if the security delivered meets requirements. Government certifications such as NIAP or DoDIN are often used to support a level or degree of security. Of course, understanding the claimed certification and its underlying capabilities is very important. The certification may sound impressive but may prove meaningless depending on the environment. How keys, certificates, encryption, and authentication are implemented and managed vary greatly. A company only stating that all trucks have bullet proof glass while driving with the back door open does not do anything for securing the cash in the truck. Companies state their featured strengths, but never their inherent vulnerabilities. It is up the buyer to find their “open back door” security vulnerabilities and assess the integrity of their security certification capabilities.

CONCLUSIONS

Every week we hear about another cybersecurity attack. National and corporate cybersecurity is the greatest threat facing the world economy over the next 10 years. Among all the myriad worries faced by global leaders, they placed cybersecurity threats above all other major concerns, reveals the 2109 EY CEO Imperative Study (Ernst & Young). While EY focused on external threats, insider threats are just as insidious. The Defense Counterintelligence and Security Agency (DCSA) constantly emphasizes the dangers of “insider threats to the country’s cleared organizations and personnel. Both must be taken extremely seriously.

With these challenges in hand, how can Security be ignored? Despite all that is going on in the world, we still hear from buyers that security is “not important”. If one looks at the big picture, security is not only important, it is strategic. This is not a tactical decision. As per EY, this is a strategic decision requiring a strategic secure platform. Is security the greatest threat to your operation? What is your weakest link? Are each and every one of your flows, including video, audio, USB, and CAC, protected with encryption? Are you using keys, and if so, are they fixed keys versus the more secure dynamic or rotating keys? Who knows your fixed key? Can users, devices, groups, and areas all be segmented and defined by the control system? Is the crypto currently FIPS certified? These questions, amongst others, should be asked of any vendor stating they provide “secure communications”.

As we look out over the next 10 years, security solutions must be able to adapt to new threats. The enemy is not standing still but continues to evolve and find new ways of intrusion. Secure platforms must be architected from the ground up with security design at its very core. It must be able to evolve and adapt. Applying security to completed applications is like putting frosting on a stale cake. Looks good, but you would not want to eat it!

Certifications need to be thoroughly scrutinized. They are not all the same. Some appear good, but in the end provide no security to your operation. Vendors that are truly secure will welcome your investigation

ADDENDUM: Security Jungle

Basic IP security terms which are important when determining the security profile of the entire system against both internal and external threats.

Encryption is the method by which information is converted into secret code that hides the information's true meaning. The science of encrypting and decrypting information is called cryptography.

Keys are used to encrypt and decrypt the transmitted and received cryptographic information. The keys provide assurance that the information remains secure. There are two types of keys: **private keys** and **public keys**.

Public key infrastructure (PKI) is a catch-all term for everything used to establish and manage public key encryption, a common form of internet encryption.

Certificates are signed by the Issuing Certificate authority (CA), which guarantees the keys. When wanting to use your public keys, you send them the certificate, they verify the signature on the certificate, and if it verifies, then they can trust your keys.

SSL (Secure Sockets Layer) / TLS (Transport Layer Security) are protocols for establishing authenticated and encrypted links between networked computers. IP address authentication is the method of identifying users requesting access to vendor databases.

SSL/TLS works by binding the identities of entities to cryptographic key pairs via digital documents known as X.509 certificates. Each key pair consists of a **private key** and a **public key.** The **private key** is kept secure, and the **public key** can be widely distributed via a certificate. The **certificate**, in addition to containing the **public key**, contains additional information such as issuer, what the certificate is supposed to be used for, and other types of metadata. Typically, a **certificate** is itself signed by a **certificate authority (CA)** using CA's private key. This verifies the authenticity of the certificate. The special mathematical relationship between the private and public keys in a pair mean that it is possible to use the public key to encrypt a message that can only be decrypted with the private key.

IP address SSL certificates secure connections directly with the submitted IP address. Via the **SSL/TLS** handshake, the **private** and **public keys** can be used with a publicly trusted **certificate** to negotiate an encrypted and authenticated communication session.

Encryption keys are created with algorithms designed to ensure that each key is unique and unpredictable. An **encryption key** appears as a random string of bits generated specifically to scramble and unscramble data. The longer the key (number of bits), the harder it is to break the encryption code.

Internet Key Exchange (IKE). IKE is a network security protocol designed to dynamically exchange encryption keys and plot the path between 2 devices. The **Security Association (SA)** establishes shared security attributes between 2 network entities to support secure communication. The **Key Management Protocol (ISAKMP)** and Internet Security Association provides a framework for authentication and key exchange. A Trusted Protection Module (TPM) can also be used to store private keys and root certificates.

Encryption Level. The most common use of encryption is the **Advanced Encryption Standard (AES**), an international standard. **AES128** and **AES256** are the two most common and support 128 bit and 256-bit keys, respectively. AES256, with 256 bits, is more secure than AES128. AES is supported by NIST for FIPS 140-2 standard. All flows, including video, audio, USB and control, need to be encrypted.

Dynamic Keys and **Static Keys** are both used for encryption. **Static keys** are fixed and rigid. These are simpler to implement, but present vulnerabilities for the entire network if discovered**. Dynamic (rotating) keys** are designed to change or rotate within a defined timeframe (set in configuration. The use of dynamic keys provides much greater security that is needed for 2021 and beyond but is more complicated.

Keys – The Importance of getting it **Right**. Proper key strategy is critical to the overall security. This is a weak link in most solutions as most systems implement a fixed key solution. Following are just a few of the risk of an improper key strategy:

There are more opportunities to get the key because it is stored on all the IPsec peer systems

- There is no way to automatically notify the IPsec peers the pre-shared key has been compromised
- Replacing the pre-shared key requires updating it on all systems, which can be tedious
- Pre-shared keys are limited to a maximum size of 64 bytes (512 bits)

Source of Keys. As keys provide access to assets, key provisioning and management are critical. Are the operating keys supplied by the vendor (poor security), or are they managed and installed by the user? The vendor should supply an initial key and certificate such that the client can provision each device with their own certificates and keys (certified third-party companies is an option in loading private keys).

Trusted Platform Module (TPM module) The private keys and CA's should be stored and protected in a HW TPM module. From the TPM module, these keys can rotate public keys (ECC or RSA). The buyer should own the process of installing private and CA's in the TPM module.

Applying Certificates. The key used to generate certificates is stored in a single location (TPM module), separate from the systems using the certificates. If not, and the certificate is compromised, all systems may be notified of a certificate's compromise via a certificate revocation list (CRL). A compromised certificate then only needs to be replaced on the system to which the certificate belongs. Certificates raise the complexity of the environment but are absolutely required.

MILS and Control System Management*).* The control system needs to be architected from the beginning for Security. It must be enterprise enabled, but also have flexibility to run in the cloud. Each and every connection within the network must also use a FIPS 140-2 certified module. Scalability, flexibility, multi cloud, open source, proven and battle tested, high speed capabilities are some of the requirements that should be embedded into the control system. The control system must be able to manage and control large, distributed networks, monitoring, auditing and controlling all aspects of security operations. Every port throughout the network from source to glass must be monitored and audited to discover intrusion, tampering or alteration. The ability for redundancy and automatic switching when failures occur must not disrupt operations. Previous generations of control systems were commonly based on Windows running on a single PC. However, with the growth of cloud computing, there are advantages for control systems to be built using microservices and containers. Kubernetes, the open-source orchestrator that manages containers is now the fastest growing project in the history of open-source software and has become very popular in IP network control systems. Within secure video distribution environments, the control system must assign access and authorization levels only by the appropriate crypto officer. MILS Access rights to devices are assigned as well as access rights to users specifying video, audio, and USB flows by classification level. Secure and authenticated connections are established by user, device, group, and areas. While the control system will enforce this, it is the responsibility of the crypto officer to set the parameters. Once the system is configured, each user can only view and engage as per their classification level. Using encryption, certificates, and dynamic key management, only the authorized user can view content. No other device nor user can view the content, unless granted by the crypto officer.

Authorization Segmentation – MILS. Multi classification within an IP platform utilizes encryption, certificates, keys, and tokens to secure the connection and ensure only the authenticated device and user can view allowable levels. The control system manages the levels and needs to support the number of classifications required. In setting up a multiclass IP operation, there can be flexibility in how it is implemented. Secure connections can be segmented by device level, user level, group level and area levels. This provides MILS implementations with tremendous number of options in assigning levels.

- Device Level will need to address individual audio, video and USB assets
- Users will need to address levels of authorizations
- Group Levels define a group of users
- Area Levels define based on user position or location
- Levels defined by unclassified, classified, secret etc.

Separate VPN's within IP switches can also be implemented to segment a single switch across multiple MILS levels. For example, ports 1 thru 23 are defined as unclassified while ports 24 thru 48 are defined as classified. Other options can include using separate switches for air gaps.

Using this authorization capability and an IP platform, users, devices, groups and areas do not have to be geographically in the same location. The flexibility of the secure environment should provide the platform to scale to campus, including remote rooms and work from home users across a secure authorized and managed network.

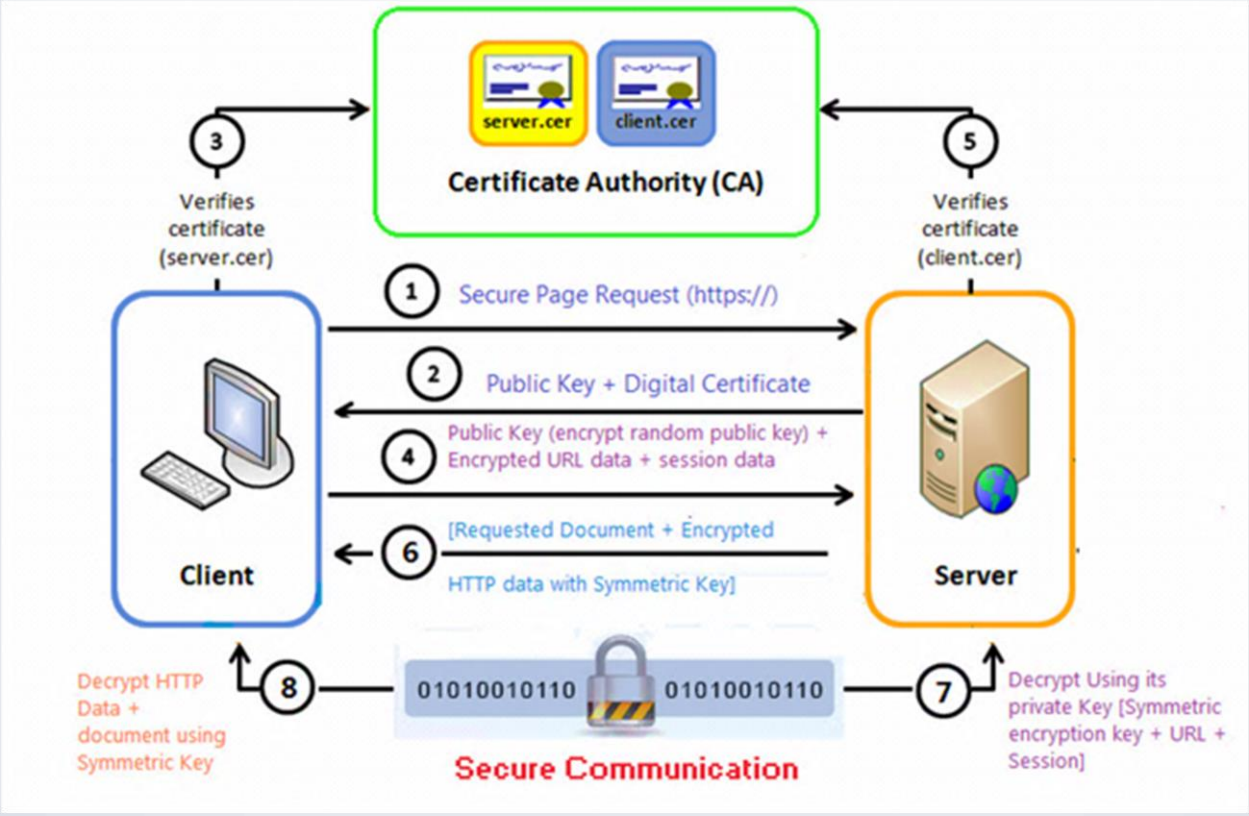


Figure 1: Securing Multiple Classifications Across a Variety of Implementation Environments
Image provided from codeproject.com

This list is just a primer on the importance of understanding your security. There are many additional factors, but without the security basics, designed into your application from the ground up, your system may be compromised. The fact that most systems today are built on legacy platforms, with "security dust" sprinkled on top of them, does not make these systems secure. Examine your installation to determine its vulnerabilities.