Grass Valley
WE LOVE LIVE

WHITEPAPER

Security in AMPP

James Westland Cain, August 2022

Introduction

We're on the internet — locked doors don't work anymore.

Historically, broadcast security has been physical. Controlled access and secured perimeters gave us the security to broadcast relying upon vetted and trusted employees with locked-down physical access to equipment.

With AMPP, Grass Valley's agile production and distribution platform: feeds, staff, production and playout (everything) — all are potentially remote. With the advent of cloud-hosted broadcasting deployments, physical security is no longer enough. With AMPP, we need a new form of security, one fit for the 21st century.

There's another consequence of this change. Just because you're inside the building, doesn't mean you can do any more than when you're at home. All actions are secured, irrespective of where you happen to be.

As secured buildings don't work anymore, we need a new paradigm. ***We need Zero Trust.***

Philosophy — Zero Trust

Zero Trust[1] is a strategic approach to cybersecurity that secures an organization by eliminating implicit trust and continuously validating every stage of a digital interaction. Rooted in the principle of "never trust, always verify," Zero Trust is designed to protect modern environments and enable digital transformation by using strong authentication methods, leveraging network segmentation, preventing lateral movement, providing Layer 7 threat prevention, and simplifying granular, "least access" policies.

Zero Trust was created based on the realization that traditional security models operate on the outdated assumption that everything inside an organization's network should be implicitly trusted.

AMPP offers URLs to the public Internet. How can we apply the Zero Trust philosophy to protect unauthorized access?

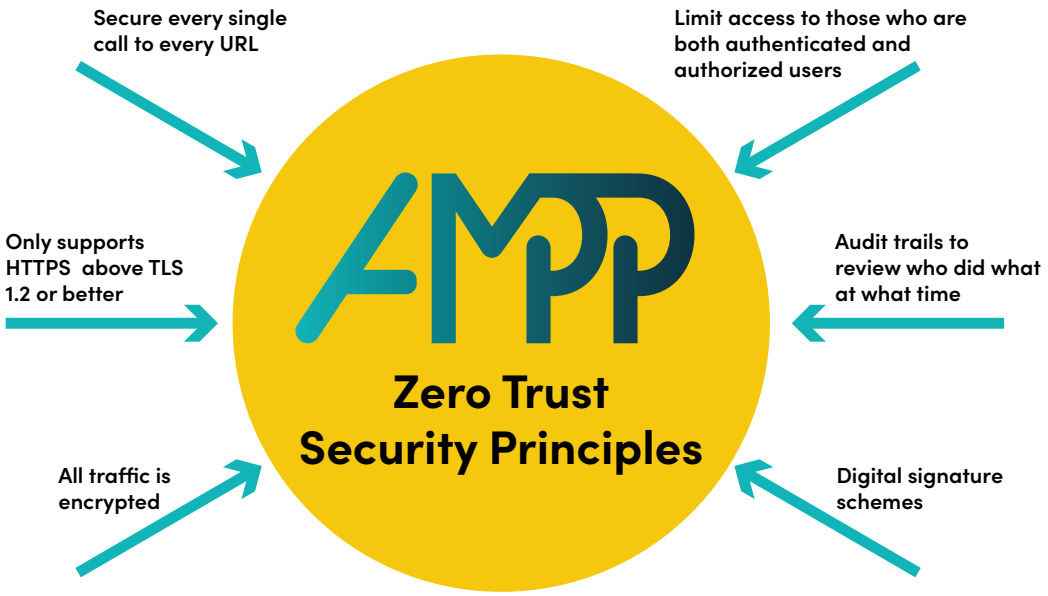

Figure 1. AMPP Zero Trust principles.

OAuth2 & OIDC

We need to secure every single call to every URL — limiting access to only those who are both authenticated and authorized. Furthermore, we need an audit trail of who did what and when.

Parts 1 and 2 of the AMWA BCP-003[2] security recommendations for NMOS APIs offer a compelling solution to these issues: only support HTTPS (when run over TLS 1.2 or better) so that all traffic is encrypted and no man-in-the-middle replay attacks are possible. Once all traffic is away from prying eyes, require that all URLs carry an OAuth2 OpenID Connect (OIDC) JWT Bearer token RFC7523[3].

A JSON Web Token (JWT) as defined in RFC7519[4] is a compact, URL-safe means of representing claims to be transferred between two parties. The claims are digitally signed by a cryptographically secure signature to ensure nothing has been tampered with. The clever thing about the signatures is that they are checkable without needing to contact the issuing authority each time.

A digital signature scheme typically consists of three algorithms:

- A ***key generation*** algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.
- A ***signing algorithm*** that, given a message and a private key, produces a signature.
- A ***signature verifying algorithm*** that, given the message, public key and signature, either accepts or rejects the message's claim to authenticity.

The JWT then has the property that the authenticity of a signature generated from a fixed message and fixed private key can be independently verified by using the corresponding public key.

This means our web server endpoints do not need to contact a single Identity endpoint when checking each HTTPS GET request. They can issue a "401 Unauthorized" quickly and independently.

Authenticating Users

Given the secure stack of OAuth2 and OIDC protecting all endpoints in AMPP, we require users to log in using their assigned credentials. These credentials can be configured inside the AMPP Identity service for small installations (where users have their passwords secured in a salted one-way hash), however, most corporate customers will have an external identity provider (such as Active Directory).

AMPP Identity can be connected to a customer's Identity Provider, to securely delegate Authentication and Authorization. All JWTs that are issued are rooted in the AMPP Identity realm however, so all external identity provider use is hidden from prying eyes. An external Identity Provider can perform Multifactor Authentication if required.

AMPP Identity can be connected to a customer's Identity Provider, to securely delegate Authentication and Authorization.

AMPP Identity has the ability to connect to Okta and AzureAD OIDC services in the same way. With an OKTA OIDC connection for example, OKTA provides AMPP Identity with a ID_Token JWT, which AMPP Identity uses to see who you are. AMPP Identity then issues an AMPP Access Token and AMPP IDToken (if requested) to AMPP clients.

Therefore, all users get security checked as they log in, where they get issued a timeboxed validated JWT. Once logged in, the software they interact with has to provide their secure JWT to each RESTful endpoint they call.

These JWTs are time constrained, so they are no longer valid after their expiration. Therefore, JWTs are constantly refreshed by all client-side libraries. If an admin embargoes an individual, this refresh will fail, locking that account from all further access.

AMPP IoT

It's not just humans that need authenticating. All AMPP Workloads are issued with Client Credential Keys that limit their access to all APIs. In the same way that a human user needs to provide credentials to be authenticated and authorized, so do all software components. Client Credential Keys can be managed from within the AMPP Identity user interface.

AMPP Workloads are issued with Client Credential Keys that limit their access to all APIs.

Encryption at REST

AMPP stores data on behalf of our customers. This data needs protected while at rest as much as when it is being transported. Hence, all data stores in AMPP encrypt their data before storing, so that even if the content of these stores is compromised, the data is useless to the attacker, who has no ability to decrypt the content.

Software Supply Chains

It is all very well making sure all data is encrypted at rest and in flight, and all actors are authenticated and authorized. There is another attack vector — compromised software.

Compromised software supply chains can infect customers just as much as compromised operational security.

If you consider all the components you need for your software, you have a long chain, and those components have dependencies, too. Any weak link can compromise the entire software supply chain, putting business at risk. SolarWinds and Kaseya are two recent high-profile examples of software supply chain attacks, and both vendors had customers that were compromised as a result.

Modern applications have hundreds of dependencies, including lots of open-source components. As developers, we don't write most of the code used in our software and applications. That can create security risks, as you can't fully control code you didn't write and maintain.

Grass Valley uses best-in-class security checks during the build process of our software. Every downloaded open-source component is checked for compromises, using auditing software that is updated with the latest CVEs (Common Vulnerabilities and Exposures[7]) — to make sure we are not accidentally including compromised software in our build chains.

This ensures that the curated software components that we offer to you are not infected with malicious or rogue components.

Our Control Plane — Your Data Plane

In AMPP, you run the software Grass Valley supplies to you. You choose which versions of each workload you run. One unique aspect of this approach is that it is easy to upgrade individual software components — our software components are loosely coupled so that most software upgrades are independent of other changes.

CVE is a list of publicly disclosed computer security flaws. When someone refers to a CVE, they mean a security flaw that has been assigned a CVE ID number.

Security advisories issued by vendors and researchers almost always mention at least one CVE ID. CVEs help IT professionals coordinate their efforts to prioritize and address these vulnerabilities to make computer systems more secure.

The CVE program is overseen by the MITRE corporation with funding from the Cybersecurity and Infrastructure Security Agency (CISA), part of the U.S. Department of Homeland Security.

CVEs allow us to discuss issues discovered by the security community — that may have impacts on software embedded in one of our deployments — that should be upgraded with urgency.

This directly aligns with best practice recommended in EBU R143[6], wherein vendors are required to inform customers of CVEs that effect their products with urgency, and offer remediation as soon as possible. With AMPP this is a matter of pulling a new version — at your convenience — and restarting that workload. This process is fully automated, and fully secured.

Don’t Take Our Word for It

SOC 2 (System and Organization Controls 2) is a type of audit report that attests to the trustworthiness of services provided by a service organization. Grass Valley is going through a rigorous evaluation by a trusted third party to be accredited with SOC 2 compliance.

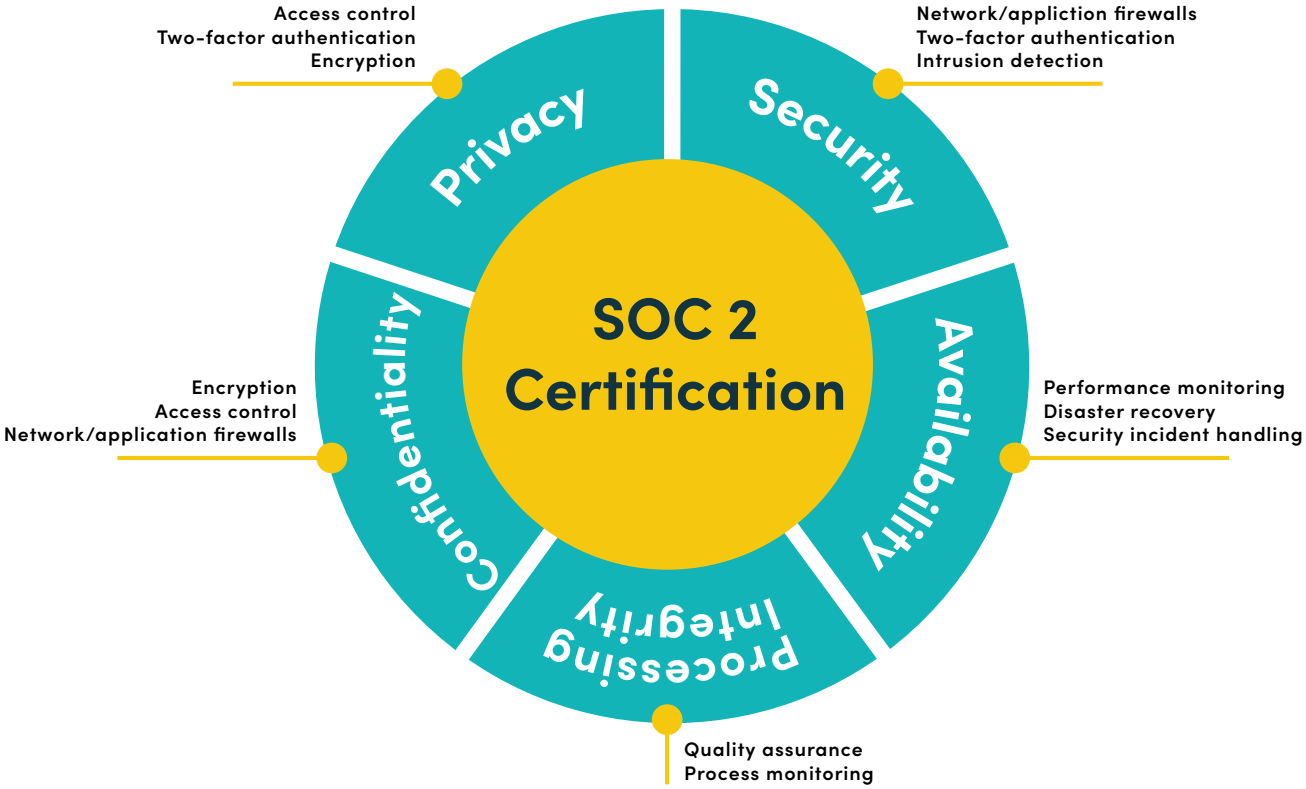

Figure 2. SOC 2 certification overview.

The SOC 2 certification process is very thorough, but it is not a one-off accreditation. It is an ongoing and constant process to keep our software services secure and our trustworthiness intact.

If you consult either EBU R143[6] or the WBU Cybersecurity Recommendations for Media Vendors’ Systems, Software and Services[5], many of the recommendations are based on good communication between vendors and customers. Good security is a constant activity that relies upon responsive organizations that communicate effectively and regularly.

Good security is a constant activity, that relies upon responsive organizations that communicate effectively and regularly.

Conclusion

AMPP has been designed from the ground up to be ***Internet First, and Hybrid*** with your on-premise deployments. By buying into AMPP, you don't have to move immediately to the cloud as it allows you to run on any kind of infrastructure, whether in your private data center, the public cloud or hybrid deployments. You can rest assured that all AMPP technologies are secure by default and rigorously tested with security in mind from the outset.

This approach means you keep your locked doors around your broadcast centers, and as you move some of your production to the cloud, you don't accidentally invite in unwanted guests!

References

1. Zero trust: https://en.wikipedia.org/wiki/Zero_trust_security_model
2. AMWA BCP-003. https://specs.amwa.tv/bcp-003/.
3. RFC7523, 2015. JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants https://tools.ietf.org/html/rfc7523.
4. RFC7519, 2015. JSON Web Token (JWT). https://tools.ietf.org/html/rfc7519.
5. WBU Cybersecurity Recommendations for Media Vendors' Systems, Software and Services, c/o NABA, 205 Wellington St. W., Toronto, ON M5V 3G7, Canada.
6. EBU R143, CYBERSECURITY RECOMMENDATION FOR MEDIA VENDORS' SYSTEMS, SOFTWARE & SERVICES.
7. CVE. https://cve.mitre.org/