Comparing Transport Access Control to IPsec

Introduction

Transport Access Control from BlackRidge Technology provides efficient and accurate authentication for Internet Protocol traffic. It is often compared to the open standard known as IP Security (IPsec). How does TAC work, and how is it different from IPsec? Can you use both methods on the same network?

Briefly: BlackRidge Transport Access Control (TAC) is more efficient computationally, protects against security issues not addressed by IPsec, and works in a broader set of network environments. Further, because each involves different layers of the Open Systems Interconnect (OSI) stack, TAC can indeed operate successfully in tandem with IPsec. TAC can run on top of IPsec without interference.

In the following sections, we first describe the BlackRidge approach, then lay out the TAC theory of operation in detail. We follow that description with a comparison of the features and operation of TAC and IPsec, and wrap up with a discussion of how the two technologies can be used in tandem.

The BlackRidge Approach

BlackRidge products take a patented approach to authenticating TCP/IP sessions which we call First Packet Authentication™[1]. It's at the heart of the TAC process.

Concept

TCP as defined [2] does not allow identity credentials to be exchanged until after a session is fully established. This design limitation exposes critical resources to attack from the Internet. You can't know whom your network is "talking to" until the conversation is under way.

Our approach, in contrast, enhances TCP— and closes this vulnerability—by using cryptographic identity tokens to authenticate TCP/IP requests *before* the session is fully established. No conversation takes place unless the party requesting a connection displays a pre-arranged shared secret as part of its initial approach.

In this way, TAC cloaks and protects network resources such as servers from network reconnaissance, port scans and many other forms of unauthorized access. Your network is a "black hole", emitting no information of any kind (not even a SYN/ACK packet) until the right to communicate with network resources is established.

TAC works with all TCP/IP based applications, and is compatible with existing networking and security infrastructure.

We'll lay out next an explanation of just how Transport Access Control works, then compare TAC to IPsec in detail.

Theory of TAC Operation

In operation, TAC generates a stream of single-use cryptographic tokens associated with the sender's identity credentials, and bound to them. When a sender initiates a new TCP session, it does so by first sending a TCP SYN packet, with a cryptographic token imbedded in the Sequence field of the TCP header of the packet. This token embodies the shared secret.

Downstream along the network path, a TAC gateway:

1. Extracts the inserted token;
2. Determines the token's authenticity;
3. Ascertains the identity to which the token is bound; and
4. Looks up the policy associated with that identity.

That security policy can then be applied or enforced.

Both for efficiency and security, a TAC gateway appliance maintains a cache of all anticipated tokens. TAC provides a constant, quantifiable level of security that is maintained independent of the number of identities and their respective tokens that are present in the system. Further, the TAC gateway resolves statistical collisions where multiple identities generate the same token at the same time.

We have also engineered in solutions to account for clock drift, clock skew and packet loss. Together, these aspects are used in countermeasures that protect against brute force and replay attacks.

A few additional notes:

- The cryptographic tokens do not directly *identify* the sender. The tokens, limited to 32 bits by the size of the TCP sequence number field, are composed solely of cryptographic hash output information. This "tagless" operation preserves the sender's privacy.
- In terms of capacity, BlackRidge TAC products have to date been analyzed at scales exceeding 100,000,000 tokens.
- BlackRidge TAC is a software solution that can operate in physical as well as virtual appliances. TAC gateway appliances are available now with 1G and 10G interfaces, with 40G and 100G products on the roadmap.

With that overview as a baseline, we'll now compare the two authentication technologies.

Comparing TAC to IPsec

Transport Access Control differs from IPsec [3] in many ways. We will focus here on five:

1. The type of platform each runs on;
2. The layer each occupies in the Open Systems Interconnection (OSI) model;
3. Interaction with (and enforcement of) security policy;
4. Interaction with Network Address Translation (NAT) and middle-box issues; and
5. Computational cost and complexity.

Type of Platform

TAC interoperates with networking and security equipment of all standard-compliant TCP/IP equipment vendors. TAC works with existing network and security infrastructures, preserving investments that have already been made. TAC can be used to communicate Identity across multiple independent administrative domains, without regard to the underlying equipment technology or vendor.

TAC is a software solution, and can operate in physical as well as virtual appliances. Further, it can be ported to additional platforms as needed, including embedded systems such as those found in ATM machines, SCADA controllers and network equipment platforms.

IPsec can be implemented in either hardware or software, with hardware acceleration being common—especially if higher throughputs are desired, in order to compensate for its computational complexity.

OSI Layer

TAC operates at the TCP/IP “Transport” Layer 4. IPsec operates at the Network Layer 3.

Interaction with Policy

TAC operates by communicating the Identity of the sender on a per session basis. An identity token is inserted by a TAC endpoint or TAC gateway, and policy is enforced at one or more policy enforcement points along the path to the network resource.

TAC policy enforcement gateways are not required to be directly connected to one another, and can be deployed without requiring all network devices to be TAC enabled. This eases migration and deployment.

IPsec, on the other hand, operates by communicating the security association assigned to the packet. Security Associations (SA) are generally provisioned on a network interface basis with each network interface being assigned a unique SA. Security Associations are usually established by using the Internet Key Exchange (IKE 2) protocol.

Interaction with NAT and Middle Boxes

TAC, simply, operates transparently in environments that employ Network Address Translation (NAT). Similarly, TAC has no interaction with, and no effect on, middle boxes.

The case with IPsec is more complicated.

NAT environments can be problematical with IPsec, which protects the integrity of IP header (in tunnel mode) and payload when using either the IPsec Authenticating Header (AH) or the IPsec Encapsulating Security Payload (ESP). The integrity is protected such that any modification of either the IP header or the payload is detectable and causes an authentication failure. Because of this, IPsec using AH does not work in environments that use network address translation (NAT), because NAT modifies IP addresses and/or TCP and UDP port numbers, invalidating the authentication.

Middle boxes can be an issue for IPsec as well. IPsec provides confidentiality to encapsulated traffic using encryption. This has the side effect of making the traffic unavailable to middle boxes such as firewalls, load balancers and network monitors. Any traffic encrypted by IPsec must be decrypted before it can be processed by any middle box.

When IPsec operates in tunnel mode, the network traffic passes through an encrypted tunnel between two IPsec endpoints. Once the network traffic exits the tunnel, it is in the clear, and any identity credentials used to establish the IPsec tunnel are no longer present.

Issues of Cost and Complexity

What about computational demands and operational complexity (and their corresponding effect on throughput and administrative costs)?

In addition to the encryption computation demands already discussed, the authentication provided by IPsec also comes at a greater cost with regard both to network configuration and load.

With IPsec:

- Negotiation is required of two separate Security Associations, one in each direction, between IPsec endpoints.
- Multiple messages are sent between IPsec endpoints to set up a single Security Association (negotiating the details related to encryption, hashing, exchange of identities, etc.). Several packets must be sent across the network in both directions before authentication is achieved.
- Network admins must configure firewalls and such to allow IPsec related IP protocols (AH = 51, ESP = 50) and ports (e.g., UDP port 500) through the network.
- The original packets are rewritten in all IPsec scenarios (AH or ESP, Tunnel or Transport), requiring the injection of new headers and rearranging of original headers within the packets. Upon arrival at their destination, these packets must then be re-parsed (and perhaps restored to their original states depending on the protocol use).

With TAC:

- Only the initial sequence numbers (ISNs) in the TCP headers are modified to contain the required cryptographic tokens. No additional headers need to be inserted, and no further modifications to the packets is required.
- A shared secret must be known to both cooperating parties, for initial session setup.
- Authentication is performed per TCP session, with the details having been pre-determined when the Identity was configured in the TAC gateways.
- For identities with pre-shared keys, no extra traffic or messaging is required to negotiate the authentication details for the packets. Alternatively, TAC can use a TLS session for secure key distribution, which may involve several packets. This dynamic identity service may be either out of band from the traffic service, or in-band.

  For pre-shared keys, no extra network configuration is required over and above what the unmodified packets would need to normally transit the network. If pre-shared keys are not used, users need to make TAC management protocols accessible to the gateways. TACs management protocols uses TCP ports 5671 and 8443.

TAC plus IPsec (Platforms and Interoperability)

When TAC is used in conjunction with IPsec, multiple TAC identities can be used within a single IPsec Security Association. These multiple TAC identities can either represent multiple independent users and devices, or composite identities that include user, application and other metadata.

IPsec can carry TAC protected traffic. When IPsec is used with TAC, the TAC identity is still present after the traffic exits an IPsec tunnel.

Conclusion

In summary, BlackRidge Transport Access Control, based on First Packet Authentication, is a robust authentication and authorization tool that offers a unique, first-opportunity security barrier to would-be attackers.

TAC can be ported to various software, hardware, virtual and embedded platforms, and provides strong, authenticable identity in all deployments while preserving the privacy of those identities.

TAC is fully compatible with IPsec, and complements it by providing pre-session authentication outside of the IPsec strong encryption environment.

Acknowledgement and References

This paper was authored by Mark Graff, founder and CEO of Tellagraff, LLC and John Hayes, co-founder and CTO of BlackRidge Technology, with contributions from Steve Hershman, Product Security Manager, BlackRidge Technology.

[1] U.S. Patent number 8346951. See http://www.google.com/patents/US8346951.

[2] RFC 793, Transmission Control Protocol (https://tools.ietf.org/html/rfc793). See also the TCP Wikipedia page at https://en.wikipedia.org/wiki/Transmission_Control_Protocol for an overview.

[3] RFC 3401 (https://tools.ietf.org/html/rfc4301) is a primary technical source for IPsec. See the IPsec Wikipedia page at https://en.wikipedia.org/wiki/IPsec for a somewhat broader view.