Hardening Operations and Management Against Passive Eavesdropping

Bernard Aboba, Microsoft Corporation

Abstract

Today within service providers protocols used for operations and management frequently send data in the clear, enabling the data to be collected by passive eavesdroppers. Examples of operations and management protocols include Authentication, Authorization and Accounting (AAA), syslog and Simple Networking Monitoring Protocol (SNMP). Since the publication of "Operational Security Current Practices in Internet Service Provider Environments" [RFC4778], the IETF has developed specifications that enable per-packet confidentiality to be applied to operations and management protocols. By developing updated operational guidance recommending deployment of per-packet confidentiality based on recent IETF Request for Comments (RFCs) and work-in-progress, the IETF can assist in bringing customer and regulatory pressure to bear in improving operational practices.

Current Practices

Today protocols for Authentication, Authorization and Accounting (AAA) are deployed for operational support of a wide range of services, including network access (dialup/broadband, VPN, wireless) as well as applications (e.g. HTTP and SIP [RFC5090]). Since AAA protocols transport network attachment as well as link layer and IP addressing information and application metadata, eavesdropping on them can disclose information useful for surveillance. This includes disclosure of information useful in determining user location, even if location is not being explicitly transported [RFC5580].

While attribute hiding is supported, the Remote Authentication Dialin User Service (RADIUS) [RFC2865] does not provide support for per-packet confidentiality, leaving operational data susceptible to passive eavesdropping. While [RFC3162] defines the use of IPsec with RADIUS, support for IPsec is not required, and to date IPsec has only seen limited deployment in service providers.

Even though the Diameter protocol specification [RFC6733] requires that "Diameter protocol MUST NOT be used without one of TLS, DTLS or IPsec", in practice many deployments do not use encryption, leaving authentication, authorization and accounting data vulnerable to eavesdropping.

Similarly, syslog and Simple Network Management Protocol (SNMP) carry a wide range of information that can be useful to a passive eavesdropper. As noted in "Transmission of Syslog Messages over UDP" [RFC5426] Section 5.2, existing deployments of syslog typically do not support per-packet confidentiality. The same is true of SNMP.

Recommendations

Since the publication of [RFC4778], the IETF has developed specifications for per-packet confidentiality of AAA, syslog and SNMP, utilizing TLS [RFC5246] and DTLS [6437]. These include specifications for transport of RADIUS utilizing TLS [RFC6614] and DTLS [draft-ietf- radext-dtls], each of which satisfy the RADIUS crypto-agility requirements [RFC6421]. Specifications for the transport of syslog via TLS

[RFC5425] and DTLS [RFC6012] have been developed, as have specifications for the protection of SNMP using (D)TLS [RFC6353] and Secure Shell [RFC5592]. Finally, Diameter security requirements [RFC6733] have been clarified.

Based on these specifications and implementations in progress, the ability to harden operations against passive eavesdropping has made substantial steps forward. It is time to recognize the need to harden operational security against passive eavesdropping by incorporating per-packet confidentiality into operational guidance.

Of course, protecting operational data sent on the wire is not enough without also protecting against unauthorized access to stored records. Operational guidance therefore also needs to recommend encryption of operational data at rest as well as controls on access to that data.

It should be understood that specifying mechanisms for per-packet confidentiality will not necessarily lead to deployment of those mechanisms, that changing operational guidance will not by itself result in improvements to operational security, and that cooperation between operators and surveillance agencies can provide access to operational data even if recommended operational security practices are in place.

However, by explicitly citing mechanisms for per-packet confidentiality as a best practice, the IETF can help in setting customer expectations, which in turn can result in economic and/or regulatory pressure for operational improvements. This can protect against unauthorized access to operational data in situations where the operator does not desire to provide access to that information.

References

[draft-ietf-radext-dynamic-discovery] Winter, S., and M. McCauley, "NAI-based Dynamic Peer Discovery for RADIUS/TLS and RADIUS/DTLS", Internet draft (work in progress), draft-ietf-radext-dynamic-discovery-09.txt, December 2013.

[draft-ietf-radext-dtls] DeKok, A., "DTLS as a Transport Layer for RADIUS", Internet draft (work in progress), draft-ietf-radext-dtls-07.txt, October 2013.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC3162] Aboba, B., Zorn, G., and D. Mitton, "RADIUS and IPv6", RFC 3162, August 2001.

[RFC4778] Kaeo, M., "Operational Security Current Practices in Internet Service Provider Environments", RFC 4478, January 2007.

[RFC5090] Sterman, B., Sadolevsky, D., Schwartz, D., Williams, D. and W. Beck, "RADIUS Extension for Digest Authentication", RFC 5090, February 2008.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5425] Miao, F., Ma, Y. and J. Salowey (Ed.), "Transport Layer Security (TLS) Transport Mapping for Syslog", RFC 5425, March 2009.

[RFC5426] Okmianski, A., "Transmission of Syslog Messages over UDP", RFC 5426, March 2009.

[RFC5580] Tschofenig, H., Adrangi, F., Jones, M., Lior, A. and B. Aboba, "Carrying Location Objects in RADIUS and Diameter", RFC 5580, August 2009.

[RFC5592] Harrington, D., Salowey, J. and W. Hardaker, “Secure Shell Transport Model for the Simple Network Management Protocol (SNMP)”, RFC 5592, June 2009.

[RFC6012] Salowey, J., Petch, T., Gerhards, R. and H. Feng, "Datagram Transport Layer Security (DTLS) Transport Mapping for Syslog", RFC 6012, October 2010.

[RFC6347] Rescorla E., and Modadugu, N., "Datagram Transport Layer Security", RFC 6347, April 2006.

[RFC6353] Hardaker, W., “TLS Transport Model for the SNMP”, RFC 6353, July 2011.

[RFC6421] Nelson, D. (Ed.), "Crypto-Agility Requirements for Remote Authentication Dial-In User Services (RADIUS)", RFC 6421, November 2011.

[RFC6614] Winter, S., McCauley, M., Venaas, S., and K. Wierenga, "TLS Encryption for RADIUS", RFC 6614, May 2012.

[RFC6733] Fajardo, V., Arkko, J., Loughney, J. and G. Zorn (Ed.), "Diameter Base Protocol", RFC 6733, October 2012.