

Security Awareness

By Adam Stone



Judging solely by the number of solutions floating around, the major Internet security issues are far from settled. Researchers made this abundantly clear on 6 and 7 February when they convened in San Diego, California, for the 10th Annual Network and Distributed System Security (NDSS) Symposium, sponsored by the Internet Society.

Papers addressed such diverse topics as security mechanisms for routing protocols, secure IP telephony, intrusion-detection architectures, and spam-deterrence structures, as presenters demonstrated that security issues are not limited to a particular specialty in the networked world.

Routing Protocols

Routing protocols present one of the thorniest problems in network security. AT&T research fellow Steve Bellovin noted at the 2002 Communications Design Conference that router algorithms are especially vulnerable to attack, insofar as they pass across and through several domains and ISPs. He and others have complained that neither the government nor the corporate communities have devoted sufficient resources to the issue.

In San Diego, however, Yih-Chun Hu and Adrian Perrig of Carnegie Mellon University, and David B. Johnson of Rice University, offered some possible help with four new mechanisms for securing routing protocols. Unlike existing techniques, these proposed solutions are based on symmetric cryp-

tographic techniques, which the authors say are about 1,000 times faster than existing asymmetric techniques.

For securing distance vector protocols, they presented a hash-tree chain mechanism that forces a router to increase the distance metric when forwarding a routing table entry. Every router presents a distance metric, that is, a distance value to a certain destination. An attacker might claim that his router offers a very short distance to some destination, thus tempting all other routers to send their packets for that destination. By forcing an increased metric, it removes the vulnerability to this kind of attack.

For authenticating received routing updates in bounded time, they offered a new mechanism called tree-authenticated one-way chains, which Perrig says are similar to hash chains. When the maximum metric is large, the technique uses skip lists — a probabilistic data structure that can be used in place of balanced trees. According to Perrig, skip lists “provide more efficient initial computation cost and more efficient element verification.” The approach is based on a new cryptographic mechanism, called MW-chains.

For securing path vector protocols, the authors offered a cumulative authentication mechanism that authenticates the list of routers on the path in a routing update, thus preventing the removal or reordering of router addresses in the list. The mech-

anism uses only a single authenticator in the routing update rather than one for each router address.

Secure IP Telephony

Recent months have seen a flurry of work on IP telephony security, which has gained increasing prominence on the enterprise IT landscape. The IETF Internet Telephony working group’s present standards efforts make the complexity of the field clear (www.ipstel.org/info/players/ietf/).

These include a specification for a basic access authentication scheme, an authentication and key agreement (AKA) based on a one-time password-generation mechanism for HTTP digest access authentication, and new functionality for negotiating the security mechanisms used between a session initiation protocol (SIP) user agent and its next-hop SIP entity.

In their work, authors Brennen Reynolds and Dipak Ghosal, both from the University of California, Davis, have taken on the threat of denial of service attacks, specifically flood-based attacks that could be mounted against IP telephony-enabled enterprise networks.

Such networks have been slow to come online thus far, Brennen acknowledged. “However, as more installations go in, more attention will be paid to the technology by both system administrators as well as black-hats,” he said. “My goal in the beginning of this work was to develop something that would be both useful and applicable to ... companies

starting from scratch as well as those with existing deployments.”

The authors’ solution proposes a multilayered protection scheme in which each layer deals with a different class of attack. The first layer of defense addresses enterprise domain authentication: all incoming and outgoing calls must be to or from users who have been authenticated by the enterprise. “Most enterprises already have this in place,” Reynolds said. “So the only additional requirements to ensure this is to allow the devices at the edge of the network (the firewall or PSTN gateway) to verify with the authentication server that the user is valid.”

‘The threat of buffer overflow is one of the more common problems that arise, and this [test] is one way to deal with it.’

The second layer of this scheme refers to authenticated control protocols. “Initially, all IP telephony protocols were untrusted and unsigned. Because of this, an attacker could easily generate malicious packets, and the target has no way of verifying that they did not come from a legitimate party,” Reynolds said. “By digitally signing each control packet, an attacker can only alter the call flow if they have compromised the key of one party involved.”

Layer three refers to data payload encryption. An encrypted payload makes it impractical to eavesdrop in real time. Layer four would add sensors for detecting and handling flood-based attacks against the system.

The authors said that using all four layers together greatly reduces the threat to the overall health of the system as well as the individual components (both machine and human). “I do not believe that these four layers of protection will completely secure an IP telephony deployment because the technology is still too new and unscru-

tinized,” Reynolds said. “But it is a very solid starting ground.”

Intrusion Detection

With ID tools an increasingly popular weapon in the enterprise arsenal, some in the research community have begun sounding alarm bells.

In spite of such concerns, or perhaps because of them, teams around the country continue to seek out new and better forms of intrusion detection. For example, Tal Garfinkel and Mendel Rosenblum of Stanford University have been crafting what they say is a surprisingly simple solution to the thorny problem of intrusion

detection architectures.

If you put an intrusion detection mechanism right up against the item being protected, Garfinkel said, you get great visibility for that object, but you also get high vulnerability. Knock out the detection system, after all, and you are right inside the heart of the system.

The alternative is network-based detection, with your detection mechanism placed in a separate box. Now you have terrific attack resistance, but visibility suffers because you’re watching network traffic instead of the computational heart of the system.

Garfinkel and Rosenblum proposed a new solution based on the advantages of virtual machine monitor (VMM) technology. By isolating the intrusion detection system within a VMM environment, they say it is possible to isolate the detection system from the monitored host. A VMM effectively puts the detection system into a different hardware protection domain, providing a high-confidence barrier between the detection system and an attacker’s malicious code. At the same time,

VMM-based detection retains excellent visibility into the host’s state.

Garfinkel said this concept can be easily put into practice today.

Buffer Overflows

Buffer overflow vulnerabilities accounted for up to half of all advisories issued by CERT over the past few years, according to University of California, Davis, researchers Eric Haugh and Matt Bishop. The two propose a new method for testing for such vulnerabilities in C programs.

Their idea is to augment traditional testing methods by instrumenting the program under test with code that keeps track of memory buffers and checks the arguments to string functions from the standard C library. If certain conditions are found, the program emits a warning indicating a possible buffer overflow flaw.

Other testing tools exist, and each handles things in a different way. “You have to decide which tool is most appropriate for the environment in which you are developing the code,” Bishop said. “The threat of buffer overflow is one of the more common problems that arise, and this [test] is one way to deal with it. It won’t work in all cases, but it may work in some.”

Looking Ahead

Bishop believes in his solution, but acknowledges the varied landscape of threats that still await remediation. The same can be said of the field of Internet security overall.

The growing use of wireless LANs, for example, has imposed some immediate security concerns, and the increasing popularity of Internet telephony ensures that there will be more work in this area. Some researchers have also begun to examine the security risks inherent in biometric technologies. Clearly, the once-neglected field of security is gaining significant attention and importance in the networked world, and researchers will continue to seek solutions to the broad range of problems we face. □