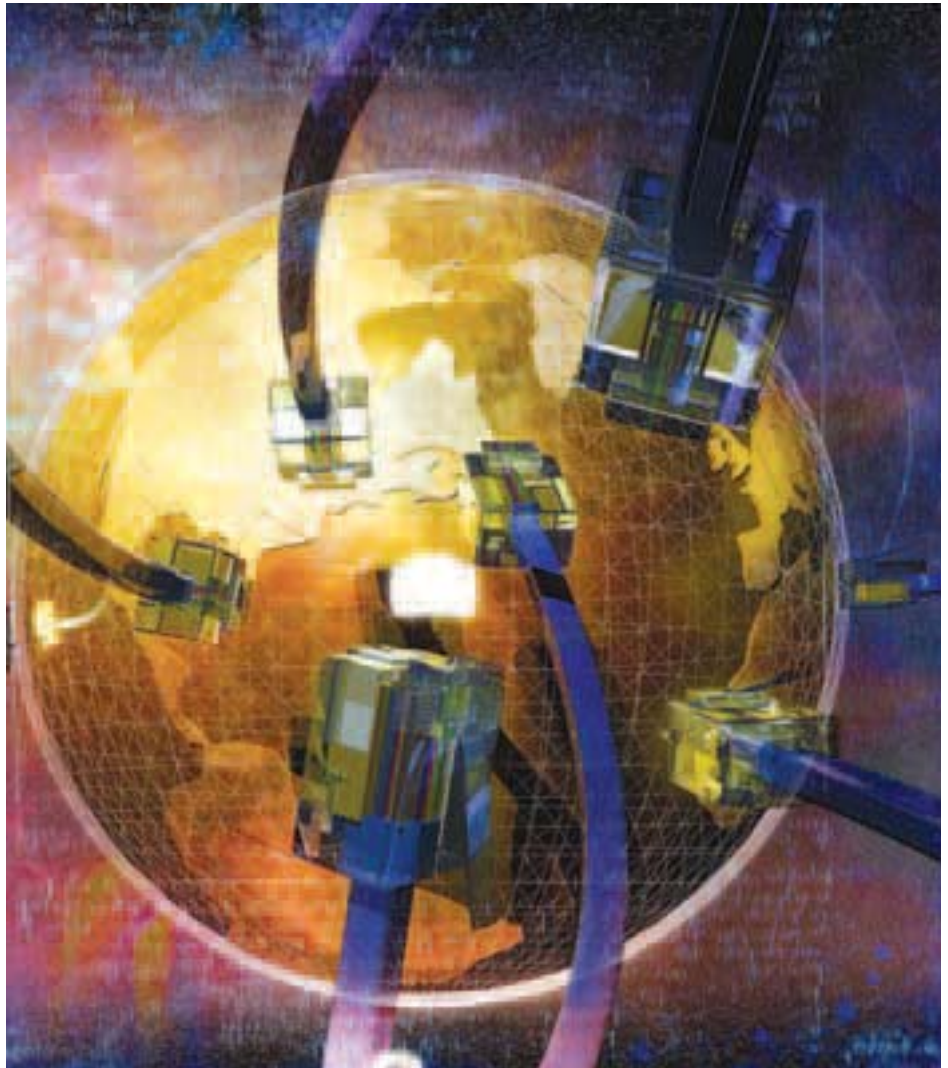


Trusted Network Technologies Uses Identity to Secure TCP/IP

The lack of digital identity at the network layer in TCP/IP has made achieving network security quite difficult.

Several protocols, such as IPSEC, SSL, and other VPN approaches layer identity on top of TCP/IP but in turn create other network incompatibilities. Trusted Network Technologies, Inc. has invented a new technology that puts identity directly into TCP/IP packets while retaining 100% backward compatibility, and they are using it to allow an identity based approach to network security.

A key weakness of TCP/IP networks is the total absence of identity at the network packet level. This leaves network layer security approaches such as firewalls to do their best to infer in real-time for each connection to a network whether the packets belong to someone authorized to access a network resource or not. The result is an near endless variety of methods to decode ever more complex high level packet data to discover what these higher level protocols say about who is trying to do what in a constantly escalating electron-



ic detective game. A game that changes with every new protocol or technique, is difficult to administer, and that is destined to fail in the long run.

Trusted Network Technologies, Inc. (TNT) has invented a patent pending method to place encrypted and digital-

ly signed identity information into TCP/IP packets while retaining 100% backward compatibility. Their first products using this approach create identity based firewalls that can provide network protection by only allowing authorized packets to reach target systems.

HOW IT WORKS

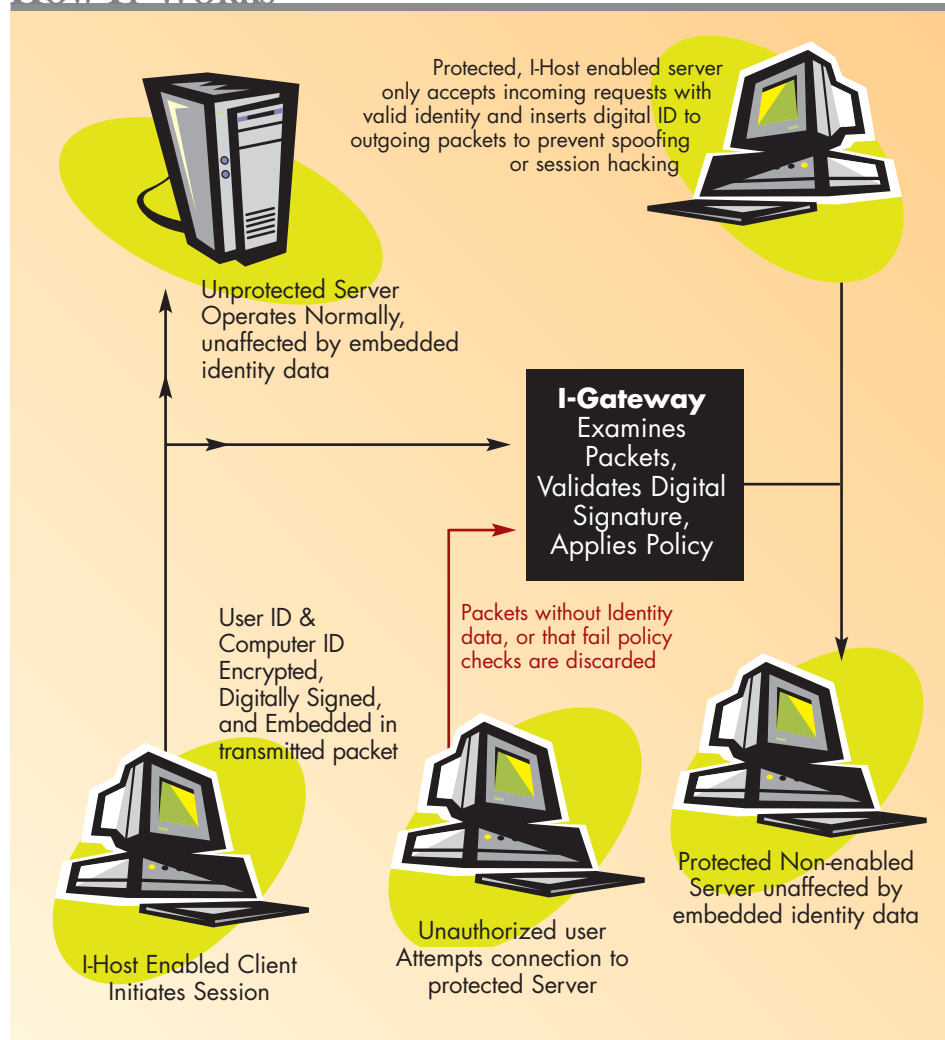
Something is Wrong

In 2002, the founders of TNT – CEO Steve Gant, CTO and VP of Engineering Dave Shay, and EVP of Business Development Derek Gant – realized that something was wrong with how the computer industry was trying to achieve network security. “The history of information security,” said Steve Gant, “is that because of the fixation on the perimeter, organizations spent an inordinate amount of time creating a castle-moat imaginary line. They built walls around their assets, not realizing that as communication became more prevalent the extended enterprise, the interconnectedness, would lead them – because of business reasons – to break down the perimeter around their organization.”

The three formed Trusted Network Technologies to create a new approach to security, one that puts identity into each user session at the network level and then uses it to create security by controlling access to network assets. They hit upon the idea of using steganographic techniques to embed user and computer identity invisibly into TCP/IP packets. This in turn allowed them to build technology that can prevent unauthorized connections to secured computers before the first packet arrives, while simultaneously logging access by both user and machine identity (which user on which machine) to aid compliance and forensic efforts. They called the resulting product Identity, and the first version shipped in late 2003.

Hiding Identity In Plain Sight

Steganography is literally the act of hiding secret encrypted writing within other, visible writing. Steganography takes its name from Steganographia a notorious book written over 500 years ago by one of the founders of cryptology Johannes Trithemius. On the surface this book appears to be about one thing (angel magic) while hidden within are encrypted messages. Steganography, then, is the act of hiding one piece of information within another. This original steganographic work was not fully decoded until 1999. *Steganography* is most commonly used in



computing to create digital watermarks in photos, music files, documents, etc. A watermarked jpeg file, for example, displays normally in a computer viewer that is unaware of the watermark, but with the proper decoding software, the watermark can be decrypted to show the origin, owner, or other encrypted information.

TNT’s products use steganography to encrypt, digitally sign, and then hide identity information in 100% RFC compliant TCP/IP packets. Because these packets are backward compatible, existing servers can accept connections from clients that place such identity information into the packets without having to know about it. But TNT’s gateway product looks for and can decode the steganographic identity information and use it to allow or deny access based on that identity and appropriate policies, without having to know

what is contained in the higher level protocols in the packets themselves.

“By being able to identify people at a very, very granular level on networks,” said Gant, “you now have the ability to move away from a perimeter centric world to an asset-centric one where every asset is surrounded by a trusted network where every user who wants to gain access to that critical asset is identified in a transparent, secure manner. Those people that do not have the digital watermark cannot be identified, and will simply not be able to connect.”

How it Works

TNT knew that the key to creating useful security was to make it easy for users to use – preferably transparent. To do this, they designed their product as three separate components. The first component – software called I-Host – is installed on each

“If we implement identity management doesn’t that mean that if a person shouldn’t be allowed to get to an application they won’t even be able to get to the machine to try to put in the wrong password?”

client computer in a trusted network. I-Host becomes part of the TCP/IP stack, and transparently adds digitally signed identity information to the packets and decodes the identity information (or lack thereof) of any incoming connection attempts. Because the identity information processing is done within the TCP/IP driver stack, the rest of the software on a client computer doesn’t need any modifications, and the use of I-Host is transparent to the user.

I-Host obtains the user’s identity information from their logon information, so if one user logs off and another logs on, I-Host will automatically change the identity information in sessions from that point on. In addition to the user identity, I-Host creates and encodes a unique machine identity from the hardware configuration. Thus each session can be identified by both the user and the machine the user is on. TNT currently supplies versions of I-Host for Windows 2000, Windows XP and Red Hat Linux clients.

I-Host only accepts unsolicited incoming TCP/IP connection requests from other I-enabled systems (i.e. it rejects connection attempts that don’t have identity information in them,) and prevents session hijacking of authorized connections between two I-enabled systems. The software is remotely distributed and installed via the I-Manager administration software. I-Host is particularized to each machine as part of installation, and thus cannot be copied for use on any other computer.

The second component in TNT’s system is called I-Gateway. This takes the form of a 2U hardened Linux based appliance that comes in versions that support 10/100 Ethernet or Gigabit Ethernet. The I-Gateway appliance enforces access policies based on each session’s identity (user ID

and computer ID.) It thus acts as an access control firewall for a trusted network segment, screening all incoming TCP/IP connection attempts. If a given connection is not from an authorized user/machine combination, then the packet is discarded and the servers on the network behind the I-Gateway never see it. The result is that unauthorized users, including even password thieves or hackers, are unable to connect to or even see machines on a protected network.

Because the identity enabled TCP/IP packets are still 100% RFC compatible, the TNT Identity series gateways can secure any type of server, even legacy systems such as mainframes. Once the I-Gateway sees that packets are authorized and allows them through to the network, servers can use them as though the identity information wasn’t present.

The third component of the TNT Identity Series system is the I-Manager which is the management interface. I-Manager performs the configuration, reporting, auditing and management functions for the system including policy creation and distribution. I-Manager itself is protected by the I-Gateway so that only authorized administrators can connect and gain access to it.

TNT’s Identity in the Real World

TNT’s product has been available for a bit less than a year, but already field experience illuminates both its current capabilities and its future potential. Certegy, Inc. is an NYSE listed global payment services provider with over \$1 billion in annual revenues. They provide credit and debit processing, check risk management, check cashing services, merchant processing and e-banking services to nearly 7,000 financial

institutions, over 100,000 retailers, and 100 million consumers worldwide. Wayne Proctor, Certegy’s CISO, installed TNT’s Identity system on his internal network to learn about the product.

Proctor had been educating company executives on identity management, and they had asked “naïve” questions that he recalled when he heard about TNT’s Identity product. “The first part of [an] identity management project is really education,” said Proctor, “to let everyone know what it’s all about. And one of the first questions [executives asked] was ‘if we implement identity management [doesn’t] that mean if a person shouldn’t get to a certain machine or they shouldn’t be allowed to get to an application they won’t even be able to get to the machine to try to put in the wrong password?’ I had to give a little education that that’s not a traditional part of identity management.”

When Proctor heard about the TNT Identity product, however, he remembered those early conversations. “When we were looking the TNT solution,” Proctor said, “we said hey, here’s a solution that you actually can – if you interface this with a standard identity management solution – keep people away to make a box invisible if they’re not supposed to be authorized to be there. That was appealing, [and] that’s how we really started to look at it.”

In November 2003, Certegy did a pilot deployment. “We deployed it in our test lab,” said Proctor. “Traditionally for best practice you shouldn’t have any connectivity of any kind between a test network and a production network. But there is always a need to send data between those networks. You could put stuff on a disk and carry it around or [use] other manual

methods, but there is always that need. What we are looking at in this first implementation [is] we know there are certain people – developers or senior system admins – that have a need sometimes to send the data across. We defined who’s allowed to send that data, what kind of protocol they can use, what machine they can send it from, and audit it tightly so if they do send data we have good audit logs of what happened.”

Managing by Identity is Different

Commenting on how the I-Gateway operates, Proctor said, “When you start actually playing with the gateway tool you start thinking to yourself, wow, this is a firewall, and it’s like it does all the same things a firewall does. But then you get that added component of the identity and the strong authentication piece that you miss out with a firewall. It’s a lot more functional than trying to twist a firewall to do what you want.” One of the first things Proctor ran into in

his pilot, however, was another difference of identity based products. The TNT product needed to be administered separately from his other identity management systems and he felt it should integrate with them. “In our small implementation it’s manageable,” said Proctor, “[But] you basically need to define [access policy] in the gateway tool per user, per system, per port. It’s heavy administration. It works great but it’s an administration burden. It’s a solid product but you really need to have the full LDAP administration and grouping [to scale to larger settings].”

So the first thing that showed up in the real world was the power that comes from making decisions based on identity. That was followed by the realization that identity based systems need integrated management capabilities focused on the identities as much or more than on the assets being secured. Policies need to be grouped by user roles and the system needs to integrate with and leverage existing identity databas-

es to be manageable at scale. The current version 1.6 released in May (after we talked to TNT customers) has evolved significantly in these directions. It now allows policies by user group in addition to individual users. Groups can also be imported from LDAP repositories and Active Directory. I-Manager now has three management “roles” so that its use can be sub-divided and delegated. Delegating the administration of identity-based systems is another requirement for administration to become scalable to larger installations.

TNT’s Identity system is an innovative version 1.x product that brings identity management to the network packet level, eliminating one of the biggest weaknesses in TCP/IP. Those who have used it rapidly realize the difference between having firewalls “make their best guess” at what’s happening with higher level protocols, and being able to truly set network access policy based on identity at the network level. ■