Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 14, Issue 2

Patent Pipeline: Securing IoT

By: Alec Schibanoff

There is a way to see into the future without a crystal ball, psychic power or a time machine. Just look at the most recently issued patents. New technologies are patented by their inventors – corporate R&D staff, university professors and students, and independent inventors – and the patented technologies of today are the technologies that will be launched tomorrow, next week, next month or next year

In this installment of Patent Pipeline, we take a look at the latest patents covering IoT security. As more and more “things” are networked together into the ever-growing Internet of “Things,” keeping those networks secure will be a greater and greater challenge. As more and more devices are added to an Iot network, the opportunity for that network to be hacked grows exponentially. And when devices from different businesses or organizations are networked together, there will need to be some type of universal inter-organizational technology that will protect the network from intruders.

We immediately think of terrorists breaking into our secure networks, and that is a genuine threat to consider. It has been assumed for years that terrorists could, for example, bring down the U.S. electrical grid, and that would leave us helpless. It was not terrorists but Mother Nature that brought down the Puerto Rican power grid, and we see the results.

In addition to terrorists, there is always the threat of hackers breaking into an IoT network and demanding payment from the affected businesses. It is, unfortunately, no longer a rare event for hackers to break into websites and past firewalls to steal sensitive data from an e-commerce business or financial institution.

And then there are competitors. For many years, it has been a common practice in Corporate America for businesses to hire competitive intelligence consultants who would – among other activities – go through the trash of competitors looking for discarded memos, business plans and other documents. Infiltrating a competitor’s IoT to find out what that company is up to is easier and far less smelly that getting it from dumpsters. Unethical competitors could infiltrate an IoT network with the goal of reducing a company’s abilities to serve its customers, damaging the company’s reputation and driving customers to the competitors.

Besides terrorists, hackers and competitors, there are disgruntled ex-employees and just plain nut cases to worry about!

Technology has been developed and patented in just the last year that addresses the threat of infiltration of an IoT network using several different approaches. Five recently issued U.S. patents show us the latest technologies and methodologies in the area of Internet-of-Things security.

Unique Identifier to Authenticate Messages

First up is U.S. Patent No. 9,319,404 for “Security for the Internet of Things.” It is the first of two patents from independent inventor Jerome Svigals, and it was issued last April. This patent includes two hardware-based and software-controlled solutions.

The invention covered by this patent includes an application control device that controls another device from a remote location. The remote device is coupled to the device that is being controlled, and it has two elements – an action portion and a security portion that contains a unique identifier. The application control device includes a rolling transaction code generator that is adapted to assign a unique rolling transaction code each time the application control device attempts to control the action portion of the remote device.

The invention can also be configured so that two or more devices communicate with each other over a network without human intervention. The system consists of a sending device that is adapted to send messages over the network to at least one receiving device, and each sending device is connected to the network via a *sending* intelligent chip, while each receiving device is coupled to the network via a *receiving* intelligent chip. The sending intelligent chip appends an "identifier" to each message that emanates from the sending device associated with it.

This identifier consists of a fixed portion that uniquely identifies the associated sending device as well as a variable portion, and the receiving intelligent chip includes a module that approves messages by validating both the fixed portion *AND* the variable portion of the identifier.

Fixed and Variable Portion Identifiers

U.S. Patent No. 9,432,378 for "Internet-of-Things Security" is also the creation of independent inventor Jerome Svigals. Granted just over a year ago, this patent covers smart devices on a network that are identified and verified by their fixed-portion and variable-portion identifiers. It is a hardware and software solution that takes the technology from his previous patent to a new level.

The invention covered by this patent consists of at least two bidirectional smart devices that are adapted to send and receive messages over an IoT network. Each smart device is coupled to the network via a bidirectional intelligent chip, logic device or other smart device. When the device is put in message-sending mode, it appends an identifier to each message that emanates from its associated sending smart device. The identifier consists of a fixed portion that uniquely identifies the associated sending smart device, as well as a variable portion that contains a secret random starting point. This secret random starting point can regularly be re-set just as a password can be re-set. The receiving intelligent chip, logic device, or smart device invokes a module contained within each intelligent chip that is configured to screen incoming messages by validating both the fixed portion *AND* the variable portion of the identifier.

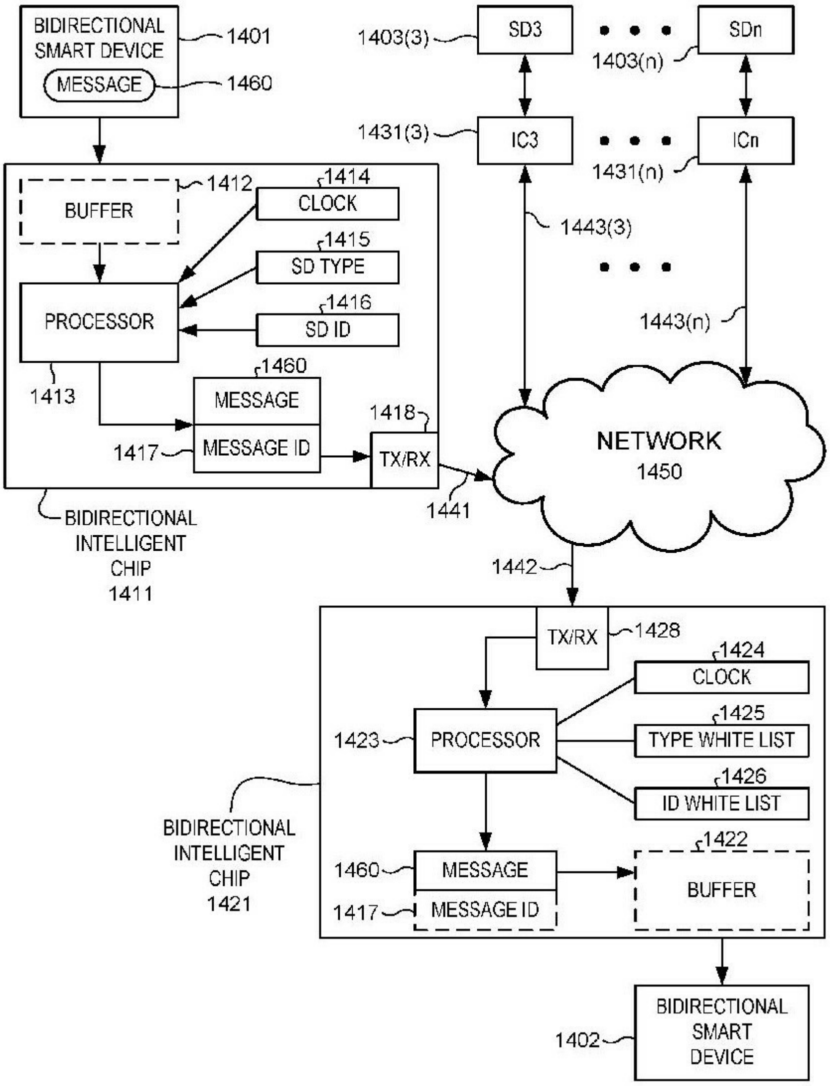

Figure 14 from U.S. Patent No. 9,432,378 provides a schematic of IoT security message flow without human intervention.

Aggregating Decrypted Data into Data Sets

U.S. Patent No. 9,479,485 for a “Network Security Method and Network Security Servo System” was issued just last year to Wistron Corporation, a Taiwan-based provider of support services for design, manufacture and after-sales services for information and communication technology products. This patent uses encrypted and decrypted data among IoT devices to authenticate them within a network, and is a software solution.

The invention covered by this patent decrypts a plurality of encrypted data points from an IoT device, then aggregates these data points into a plurality of aggregated data sets so the aggregated data points form a plurality of data sets. It retrieves centroid data points corresponding to the data sets so that the first centroid data points form a first core data set. It then retrieves a second set of centroid data points that correspond to the first core data set and a second core data set in which the second core data set corresponds to other Iot devices. The system determines if the IoT device is an anomaly state based on the second centroid data points. It can then isolate a specific IoT device to a specific virtual network when it determines that an IoT device is in an anomaly state in much the same way that anti-virus software isolates questionable files on a hard drive. Once a suspected device is verified to be authentic, it can be released from isolation and returned to the network.

Testing Transaction Protocol to Verify a Device

U.S. Patent No. 9,510,195 for "Secured Transactions in Internet-of-Things Embedded Systems Networks" was also granted last year to the Dutch semiconductor giant, STMicroelectronics International N.V. In a world of man-to-machine and machine-to-machine interfaces, it is important to note that the technology covered by this patent is totally machine-to-machine and does not require a human interface! It is a hardware solution that uses an integrated circuit that is separate from the network to verify communications within the network by testing the integrity of the transaction's protocol.

The patent creates a secure network-enabled device and a second security module that is an integrated circuit. The security module is initiated, and data is communicated from the secure network-enabled device via a transceiver. The security module is configured to test a subset of the data communicated to the secure network-enabled device, and the security module is configured to test the integrity of the transaction protocol that governs the stream of data bits of the data communicated to the secure network-enabled device. If the protocol does not match the established standards for the network, that device is not permitted to communicate with other devices in the Iot network. At that point, human intervention is needed to over-ride the system when it produces a false negative.

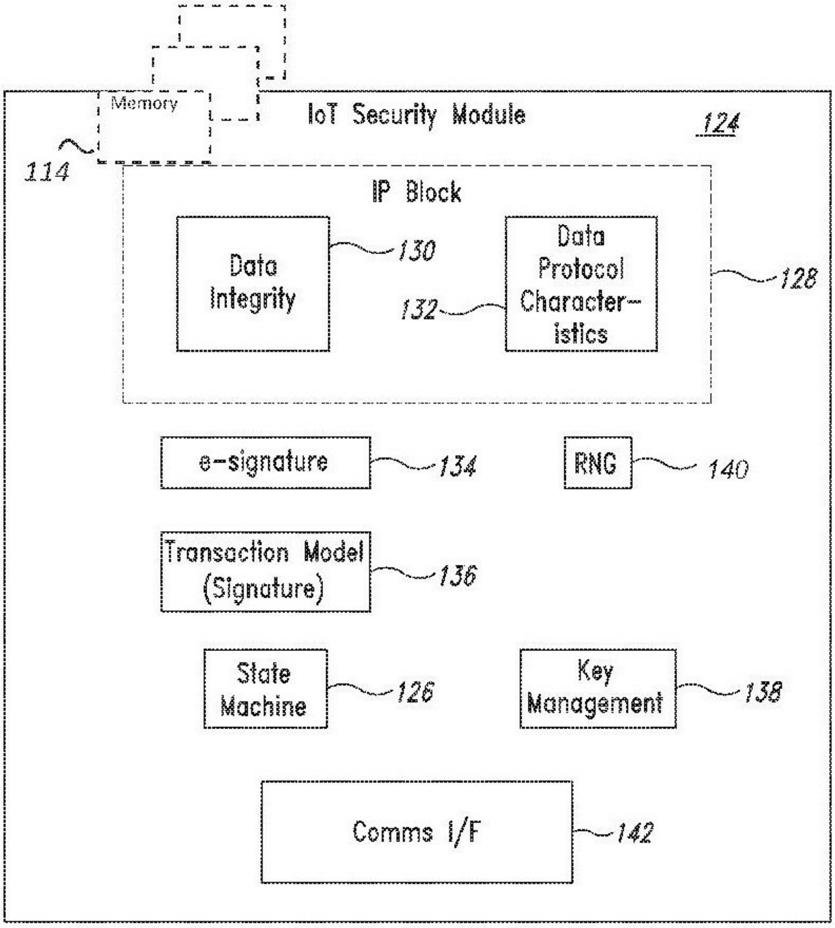

Figure 4 from U.S. Patent No. 9,510,195 is a block diagram of an IoT security module.

Digital Token that Decrypts a Digital Certificate

U.S. Patent No. 9,716,595 for a "System and Method for IoT Security and Management" was issued just this year to T-Central, Inc. Doing business as "TrustCentral," T-Central designs and develops online security solutions, specifically security architecture for mobile platforms. This patent uses software to create a digital token that decrypts digital certificates assigned to devices on the IoT network.

The invention covered by this patent begins with the establishment of secure communications between devices in an IoT network, followed by the issuance of a digital certificate to one device in the network that invites a second device in the network to communicate with it by receiving a digital token that is authenticated using a unique identification and cryptographic key of the second device. It then establishes a secure communication line between the network devices by authenticating the established communication line and issuing a second digital certificate to the communication line. This prevents a device that does not have a digital token from establishing secure communications with devices in the network because they will not be able to identify the cryptographic key of the devices' digital certificate.

Good News for IoT Network Operators

While keeping an IoT network secure is – and will continue to be – a challenge, there are numerous solutions that address the issue. The technologies covered here will be but a few of the solutions to come to market in the next year or so.

Alec Schibanoff is Vice President of IPOfferings LLC, a leading patent broker and IP consulting services firm, and publisher of the Patent Value Quotient. Mr. Schibanoff also serves as Executive Director of American Innovators for Patent Reform, a trade association that represents businesses, universities and the IP community, and advocates for stronger patent laws and more vigorous enforcement of patent rights. He is the author of dozens of articles on patents and intellectual property-related issues. He can be reached at alec@IPOfferings.com.