Multifactor Authentication – A New Chain of Custody Option for Military Logistics

Tom Waters

ABSTRACT

"An Army Marches On Its Stomach," is a quote attributed to both Napoleon and Frederick the Great.[1] Both men certainly would attest to the veracity of the sentiment—without secure supply lines, no army can survive for very long. This reliance has grown beyond mere food and now encompasses a broad range of materiel from pencils to remotely piloted drones.

By their very nature, military supply chains are a high-value target for thieves, saboteurs, and counterfeiters. Fraudulent materials, particularly those switched out for high-grade defense aerospace technologies, represent a serious risk to military operations. When materiels that can't meet military standards fail in combat situations, it is the warfighter or the innocent bystander who pays the price.

Two-factor authentication has emerged as a reliable metric for mobile device security. What began with only a small smattering of authentication dimensions is now morphing into a range of options that, properly considered, will provide logistics personnel with the necessary assurances their authentic cargo is delivered safely.

Military freight must often pass through multiple civilian supply chain way points, from maritime freight to industrial warehousing, to 'last mile' delivery at forward operating bases by contractor personnel. This creates numerous opportunities for shipment interception, tampering, and replacement.

Counterfeit materials, particularly of aerospace and communication components, represent a significant threat to military operations when these fraudulent supplies don't meet military specifications.

Tom Waters leads a small intelligence team for a Fortune 200 corporation, crawling behind Silicon Valley's headlines to research the global tech market–mobile devices, autonomous vehicles, social media, data analysis, streaming technologies, and e-commerce. He previously served undercover for the Central Intelligence Agency, helping protect U.S. technologies and intellectual property from theft by foreign agents.

Tom has been a guest lecturer at the Naval Post Graduate School, the University of South Florida, and Johns Hopkins University. He is also a popular speaker at technology conferences in Silicon Valley, New York, and the UK. He holds several patents on digital authentication technologies and is the co-inventor of Transactional Key-Pair Encryption, a new Public Key protocol for the quantum computing age.

BACKGROUND

Two-factor authentication has reduced incidences of fraud, including identity theft, in e-commerce. Consumers are no longer at high risk from thieves due to the compromise at a single point of failure in a transaction. Two factors–for a Personal Identifier Number (PIN) and an RSA token–are force multipliers, dramatically improving the security of online transactions.

An explosion of mobile phone applications, or apps, are taking advantage of these technologies. And in doing so, we're seeing innovative new options for increasing the force-multiplication of multifactor authentication. Supply chain and logistics software can leverage these technologies. The potential for protecting military supplies from theft or counterfeiting is in its infancy, but the potential savings, in time and treasure, are considerable.

JUST IN TIME DELIVERY

For years, online retailers like Amazon have had robust, networked systems in place for orders, shipping, and delivery. What began with the simple delivery of books has expanded into an array of skillfully delivered expensive electronics, fashion items, and even wine. These brands are highly coveted, exclusive, and expensive—making them ripe targets for counterfeiters and thieves.

Amazon and its myriad of copycat imitators have changed the logistics industry in ways no one could have imagined. These increasingly predictive systems have in turn spurned new research into the art of the possible for supply chain vendors. With the coming advent of smart-packaging, materials can know where they are and what conditions they've experienced along the way. Supply chain-of-custody software applications can be designed to provide complete end-to-end authentication, ensuring that what is delivered is the actual item that was ordered.

Two-factor authentication originally formed around three basic credentialing criteria; *something you know, something you have,* and *someone you are.* These are relatively straightforward to implement at the desktop PC level.

- *Something you know* – a PIN or Password created by you
- *Something you have* – an RSA token or other hardware keyfob assigned by an authority
- *Someone you are* – a biometric sensor registered as you

Two-factor authentication has existed for secure communications systems for years. But moving the process to a mobile environment provided some unique challenges before specific solutions were introduced.

Tokens and USB-based key fobs for PC access are fine—but people do not want to have to carry them around to use with a mobile phone. There are few plug in ports for USB's, and RSA tokens are inconvenient when one hand is already dedicated to holding the smartphone. Taking both outside, away from office environments, provides lots of opportunities for loss, driving up costs and increasing delays in accessing systems. Fortunately, innovation followed mobility.

Each mobile phone has a number assigned to it–several numbers in fact. There is the phone number someone calls to reach the phone's owner. That requires a government identification and some method of payment, generally, a credit card billed to that person.

There is the SIM card the carrier uses to identify the phone owner's account. SIM cards can be swapped between devices to use a single data subscription plan on multiple devices. They carry a small amount of data on board, with varying degrees of security, and some can store credentials for credit card purchases. [2]

There is also the IMEI, the International Mobile Equipment Identity number, a fifteen-digit number used by cellular networks to identify specific devices on the network. But the IMEI is only utilized for the smartphone device, the hardware. It provides no insight into the user and whether or not they have the authorization to use the device.

So on the surface, one might think that these three numbers would be adequate to authenticate a user. But between the cloning of a cell phone number, the hot-swapping of SIM cards between devices, and the singularity of hardware-specific IMEI the basic ease of stealing the information remains. There's an old saying in cybersecurity—amateurs try to break the encryption, while professionals just steal the keys. The phone number, SIM card, and IMEI are those keys, and all are reasonably easy to steal in one way or another.

This is why fingerprint sensors came into general use. There is a common misconception that the sensor takes a photograph of the fingerprint image and stores it on the device for comparison when a new fingerprint is presented for comparison. But this is incorrect—the accompanying software turns a fingerprint's pattern of whirls and loops into a mathematical algorithm. When authentication is requested, it compares the mathematical score of the newly presented fingerprint to the one stored on file. If there is a statistically significant match, the phone is unlocked.

Fingerprint scanners are reliable and have brought new security to mobile devices. Apple based the 2011 debut of their Apple Pay online service to the fingerprint scanner, and Android devices quickly followed with their sensors. Fingerprint authentication is now widely accepted for payments from vending machines to Uber rides across town. It improved trust and reliability in mobile devices as financial tools. This, in turn, has spawned an industry of developing applications that can leverage and expand this trust model.

NEW MODELS OF AUTHENTICATION

The field of potential authentication technologies that are available on smartphones and other devices commonly used by military and civilian personnel are exploding, with new types and dimensions coming online regularly. Among these are:

Location Proof

Using the GPS chips in modern smartphones, logistics planners can simply and securely know when a package has passed from one part of the supply chain into another. This could be a pallet offloaded at a port, or a single package being dropped off via courier. In either case, capturing the GPS coordinates from a consumer device creates yet another layer of security in a chain of custody.

Possession Proof

Radio Frequency Identification (RFID) technologies have been around for years, and are common in industrial and warehouse settings for on-location use. Smartphone technologies have now improved to where systems can incorporate RFID chips on shipped materials. Smartphone cameras can take pictures of Quick Read, or QR codes frequently used by national shipping companies like UPS or FedEx. These commercial applications have significantly reduced the costs of the associated hardware and software, spinning off a litany of third-generation software applications useful to the military.

Access Proof

Many consumer smartphones have data plans with very high fees. For this reason, users are often highly selective of which smartphone applications they allow to access a cellular-based data plans. For these users, local Wi-Fi is a cost-effective option for by passing expensive cellular plans. Corporate providers of shipping and logistics services can use this technology as another dynamic layer of security. Allowing someone onto their Wi-Fi, or company IP address provides another proof-of-authority in a multifactor environment.

Proximity Proof

QR Codes and RFID are fine for pallet and package authentication. But what if supply chain officers want to confirm proximity to other military hardware? Pilotless drones, autonomous vehicles, or delivery robots can utilize short-distance communications technologies like Bluetooth or ZigBee to authenticate a close (3-5 feet) exchange of materials that can easily be captured and archived.

Behavioral Proof

Behavioral biometrics is the latest iteration of authentication technologies, and likely will be one of the hardest for bad actors to crack. The way each of us signs our name is unique. Though a bad actor could trace a legitimate signature over a capacitive-touch screen tablet, all it could do is reproduce the final image.

The speed of motion, change of direction, curvature of the letters, and even the pressure applied with a stylus pen is unique to each person. Like a fingerprint sensor, signature authentication stores a unique mathematical algorithm. The behavioral requirement to reproduce it creates a unique, on-demand authentication dynamic that has a high degree of reliability.

Confirmation Proof

Sending a one-time text to a cell phone number associated text message system or email address is an increasingly common authentication vector. These one-time codes are easily archived and associate with the individual tied to that number and (messaging or email) service. Many U.S. banks have adopted this for confirming mobile-device access to financial accounts and services.

Witnessed Proof

Among their other similarities, a common denominator between drones and smartphones is the ubiquitous use of cameras. Smartphone camera quality has been rapidly increasing over the past few years, and even low-cost units can now rival some SLR cameras for picture quality.

From sporting events to criminals caught in the act live, consumers are recording moving images and broadcasting them worldwide. This same technology can also be used as a type of video-centric Notary Public, where the handoff of a particular cargo can be captured from the air or surface and archived permanently.

Radio Proof

A new technology that is ‘available’ but disabled on most smartphones is an FM radio chip. Several unique dual or multi-channel authentication strategies are possible if carriers and manufacturers chose to activate this component. Fortunately, once that decision is made, a simple over the air software upgrade will enable the chip to work again. (The same process Tesla uses to upgrade the software on their cars.) [3]

These different modalities, taken together, provide a unique and dynamic authentication environment for DoD supply lines. Authentication doesn't have to follow a standard (read: predictable) playbook. It can adjust on the fly, requesting different proofs based on environment, timing, classification, risk, and operational complexity.

What's more, the database-friendly nature of these technologies opens an array of modeling options. While a 'central' database structure is preferable under a typical commercial model, military planners can use distributed databases that are linked together for data sharing purposes. In doing so, not only is the data automatically backed up, but it can also be mined for a variety of fraud detection purposes.

Statistical regression and other analytical techniques can be performed in near real time looking for commonalities where cost saving measures can be applied. They can also search for outliers, evidence of anomalies that need to be investigated while the potential perpetrators are still in theater. These could identify insider threats (theft), external actors (counterfeiters), and organized hackers (state or non-state criminal elements).

This 'Supply Chain of Custody' superficially resembles a block chain, but it's nothing of the sort. Block chain is a distributed authorization system, whereas this is a distributed participation system–one built around a centralized DoD authority (i.e., the military maintains control). Military elements could share information across services, from regular forces to SOF elements, and from full-time service personnel to Reserve units quickly and securely. It also assists in the final disposition of military items–either disposed of in theater, returned via military channels, or shipped through contracted commercial vendors. A chain of custody remains in place for the materials from cradle to grave, eliminating military surplus from falling into the wrong hands.

CONCLUSION

Military leaders will not need to be convinced to 'try' these options; they will welcome the opportunity to add authentication, authority, and auditing tools to their supply chain. The cost of application development is not quite commodity-level yet, but it is getting closer every day. The ability to share information from forward elements, to rear echelon, to HQ elements, to commercial suppliers has never been easier, more cost effective, or secure.

Military personnel frequently use ride sharing applications like Uber to get from one place to another. Platform software applications like this provide bona fides within the system itself, protecting both the driver and the passenger. They are simple, well designed, secure, and accepted by members of the civilian and military population.

There is no reason logistics planners can't use similar software platforms to increase their efficiency, reduce waste, and prevent fraud from interrupting supply lines using the same technology. Multifactor authentication is the future of logistics, and military planners can be among the first to benefit.

NOTES

1. Defense Procurement International 2011; Camp and Base Solutions; "An Army Marches On Its Stomach", accessed April 30 2017 from http://www.electrothermal.com/adminimages/Electrothermal_editorial.pdf.

2. Daniel Bader, "What is a SIM Card and What Does It Do" iMore (Online Magazine), accessed on April 30, 2017 from http://www.imore.com/what-is-sim-card.

3. Alex Brisbourne, "Tesla's Over-the-Air Fix: Best Example Yet of the Internet of Things" Wired Magazine February 2014, accessed April 30, 2017 from https://www.wired.com/insights/2014/02/teslas-air-fix-best-example-yet-internet-things.