Identity Content Assurance and Tracking Systems (ICATs) for Military Supply Chain Risk Management: A Preliminary Design

Raymond R. Panko
University of Hawai‘i
Panko@Hawaii.edu

Abstract

Military supply chains are vulnerable to counterfeiting in hardware, software, and medical supplies. This paper sketches an approach for placing identity content on supply chain items. This approach would protect this identity content with cryptographic digital signatures. It would involve testing digital signatures on arriving items, tracking items over their life cycles (including counterfeit detection at each stage), and sharing information about detected counterfeits—especially if the counterfeiting suggests sabotage by a national adversary.

1. Counterfeiting threats to the military supply chain

Counterfeiting is an issue for all supply chains. For military supply chains, counterfeiting is a special concern because a small amount of targeted counterfeiting can create disproportionately large damage war fighting capabilities.

Recently, the U.S. Government Accountability Office [10] reported numerous counterfeiting instances in Department of Defense Systems, including the following:

- A large number of counterfeit routers were found in military networks. If these had failed around the same time, the consequences could have been debilitating.
- Counterfeit oscillators for ground-based GPS systems were discovered in Air Force and Navy systems. More than 4,000 different military systems use these oscillators for critical positioning information.
- The U.S. Air Force bought four counterfeit microprocessors for the flight control computer in F-15s. Fortunately, suspicious markings on the parts caught the attention of installers, and the counterfeit microprocessors were not installed in the aircraft.
- In a somewhat related area, NASA had to delay a probe project in 2009 for nine months and went 20% over budget because of a single counterfeit part [6]. In other words, counterfeiting does not have to be widespread to do serious damage.
- Of course, examples like this do not prove that there is a serious overall problem. To get a better estimate of the magnitude of the counterfeiting risk in military supply chains, the Department of Commerce [8] surveyed 387 suppliers and DOD organizations about counterfeit hardware components. These organizations reported a total of 3,868 counterfeiting incidents in 2005 and 9,356 in 2008. (An incident could involve a single part or a large number of parts.) For parts on the critical Qualified Products List, the number of reported incidents rose from 11 in 2005 to 110 in 2008.
- In addition, most reported counterfeit components were found because they were poor copies visually or because they simply failed or never worked at all—not because they were discovered in proactive anti-counterfeiting programs. The real counterfeit incidents rate at each firm may have been much higher.
- Also, the Department of Commerce study noted that because detected counterfeits typically are not reported or entered into accessible databases, there is no way to know even the true magnitude of detected counterfeits today.
- Despite these measurement weaknesses, government officials believe the problem to be extensive. One DOD official estimated that counterfeit parts create a 5 to 15 percent annual decline in weapons system reliability [5].
- Based on the description of counterfeit incidents, the motivation for most of the counterfeiting found in the Department of Commerce [8] study appeared to be simple greed. Traditional methods for deterring criminal product counterfeiting are likely to be applicable for this type of counterfeiting.
- However, military supply chains must also deal with another motivation for counterfeiting—sabotage by national adversaries. For example, there is
considerable evidence that China has engaged in widespread cyberespionage against the United States [7], and China was by far the source of most hardware counterfeiting incidents reported in the Department of Commerce [8] study. It would not be difficult for the Chinese military, rather than financially motivated criminals, to inject selected counterfeit components into the U.S. military supply chain. Both the Department of Commerce study and the Government Accountability Office [10] study indicated that the controls needed to detect sophisticated counterfeiting are at best inconsistent in quality.

Sabotage through counterfeiting has a long tradition in military conflicts. During the U.S. Revolutionary War, the British flooded the U.S. economy with counterfeit Continental Congress bills [1]. This thoroughly debased the currency. After the war, the U.S. had to return to coinage instead of paper currency. In World War II, the Germans created 9 billion counterfeit British bank notes worth more than 134 million British pounds; they began to flood the British economy in 1943 [2]. Had the Germans succeeded in distributing this currency fully, financing the war would have become extremely difficult for Great Britain.

Microprocessors are special concerns for electronics counterfeiting. Microprocessors are the most frequently counterfeited microcircuits [8]. If a sophisticated attacker can inject fake microprocessors into the military supply chain, these devices could be built to include disabling circuitry if certain events occurred or circuitry that causes subtle errors if given events occurred. The GAO study [10] indicated that reverse engineering is frequently used to create counterfeit electronic components, so microprocessors with hardware logic bombs should not be beyond the production capabilities of national adversaries.

Counterfeit software could do sabotage even more easily and in far more sophisticated ways. This was only fiction, but event-based sabotage is a serious potential risk for military supply chains. Disgruntled employees have long placed software time bombs or event-specific logic bombs in corporate software [4]—sometimes with disastrous results. National adversaries have far more resources to do sabotage. In addition, injected software routines could be large and complex compared to malicious circuitry likely to be built into Trojan horse microprocessors.

Counterfeiting in the military supply chain could also extend to drugs. Counterfeit drugs are a very serious concern worldwide [11]. Again, the main motivation for medical counterfeiting today appears to be greed stemming from the high prices of individual pills and other dosages. However, sabotage could be important if national adversaries could inject disabling medications into the military supply chain if conflict began or if the effects would not be discernible quickly. In fact, even if effects were immediate, the source of the attack might be untraceable. There currently are many technical ways to make drug counterfeiting more difficult [9]. The military only deals with a few drug suppliers, so the targeted injection of malicious drugs into the military would not be prohibitively difficult. For instance, Pfizer has been using RFID tags with Viagra since 2006.

2. Identity content assurance and tracking systems (ICATSs)

To reduce the risk of sabotage through counterfeiting, the U.S. military supply chains need improved ways to detect counterfeits at each stage of each supply chain. There will be no silver bullet for doing this. However, we will describe at a high level one potential comprehensive countermeasure system that we call the Identity Content Assurance and Tracking System (ICATS). ICATS would apply cryptographic security to item identification and tracking. This method could be used as a component in general anti-counterfeiting programs in military supply chains.

ICATS would include a tracking system. Tracking systems allow any party in the supply chain to trace the “provenance” or “pedigree” of an item from production through each step in the supply chain. This provenance information is critical in detecting counterfeits. In one case, the military discovered that a helicopter component had the same serial number as one listed as scrapped. Closer inspection determined that the part had been retrieved from scrap and welded back together. Yet few parts tracking systems are in place.

The tracking system for individual parts needs to be linked to databases of counterfeit items and items that are suspected of being counterfeit. If an item is caught by any member of a supply chain, inputting information into a counterfeit parts database would alert other supply chain members who might have purchased the same item.

3. Content assurance paw prints

When a part arrives, it would be useful if certain information about its identity came attached to it. A simple example of this identity information would be a part number and serial number. Currently, the U.S. Missile Defense Agency requires serial numbers on all items costing over $5,000 [10]. However, these numbers might be inscribed in ways that were possible to replace or copy. In particular, national adversaries
might not find the addition of false serial numbers to Trojan horse electronics parts to be a significant barrier.

In general, we will call the information to be assured the identity content (IC). In this example, the identity content is a simple part number and serial number. However, there is no limit to the length of identity content. The IC, for example, could include technical specifications and other information valuable in actual use and to prevent counterfeiting. It could even include information needed for non-authentication purposes, perhaps even including a use manual.

ICATS would require a product marking system that offers military-grade strength in authentication and integrity. Authentication means that the source of the identity information can be determined. Integrity means that if the identity content is changed after the original producer places it there, this tampering will be easily, quickly, and reliably detected.

The strongest form of cryptographic authentication is a digital signature signed with the original creator’s private key. We call the combination of the content and the digital signature an ICATS paw print. To check the paw print, a verifier in the supply chain would test the digital signature with the public key of the originator. (Caveat: The discussions of digital signatures and certificate checking in this paper are simplified. See Panko [4] for a more complete discussion.)

3.1 Creating paw prints

Figure 1 shows how to create a paw print. The originator “signs” the information in the paw print. This means that the originator treats the identity content as a stream of bits and encrypts this bit stream with its own secret private key to create the digital signature. It adds the digital signature to the protected information to create the paw print.

As a further level of protection, the paw print could be encrypted for confidentiality using a symmetric session key. This protection is not discussed in this paper.

3.2 Testing paw prints

Figure 2 shows that the verifier needs to know the public key of the originator to test the paw print. In contrast to the originator’s secret private key, the originator’s public key is non-secret and is widely available. However, the only secure way to get the originator’s public key is to get the originator’s digital certificate from a trusted certificate authority (CA).

The digital certificate has a number of fields. The two most important are the name of the digital certificate’s subject and the subject’s public key. If you
Figure 2: Testing the paw print

want the public key of company XYZ, you contact a trusted certificate authority that maintains XYZ’s digital certificate. You then read the public key in the certificate.

Another important field is the digital certificate’s own digital signature. The digital signature is created by the certificate authority with its own secret private key. The person receiving the digital certificate can test this digital signature with the well-known public key of the CA. The person receiving the digital certificate should also check with the CA to discover if the digital certificate has been revoked before the termination date on the digital certificate. ICATS would do all of this automatically.

The verifier then decrypts the paw print with the public key of the originator. If the originator created the paw print, and if the paw print has not been altered, the decryption will produce the identity content (or the hash of the IC). This can be compared with the paw print’s actual content (or hash). The two must be equal for the part to be accepted.

If a counterfeiter who does not know the originator’s private key creates a fake paw print, then decrypting the false paw print’s digital signature with the public key of the true producer will not give the content information. If there is no match, the part is rejected. This process will also detect if a counterfeiter changes the protected content information (say to give it the part number of a higher-quality part). So ICATS uses public key/private key encryption and a digital signature to create authentication. This also provides message integrity.

However, authentication is the hardest part of cryptography because authentication processes always makes certain assumptions. In the case of digital signatures, for instance, the whole process fails if the counterfeiter can learn the originator’s private key. Consequently, private key protection is a critical issue in any real ICATS system.

More subtly, the counterfeiter may be able to simply copy the paw print onto many counterfeit products. As we will see next, the purchaser can partially defeat this by checking the pedigree database that is part of ICATS. The check would reveal duplicate parts with the same part number and serial number.

To counter this, a national adversary wishing to counterfeit a microprocessor can create a single microprocessor with Trojan horse instructions and copy a product name/serial number paw print to this single counterfeit microprocessor and destroy the original product. In that case, a check of the ICATS database will not reveal the fraud.

This ploy, fortunately, can be defeated with more complex paw prints. For instance, if a splash of ink (which we will sadly call a hairball) is shot onto each part, computer pattern recognition like that used in iris recognition could add a component to the protected content information. Copy-resistant methods like those used to prevent the photocopying of paper money and tamper-evident protection like that used in driver’s licenses could be used to protect the hairball.

In authentication, there is always a war between impostors and verifiers. The goal is to create authentication measures that are prohibitively expensive to defeat. Of course, national adversaries are motivated to invest heavily to inject highly damaging counterfeit systems into the supply chain.

We should also note that the digital certificate approach requires the creation of a full public key infrastructure (PKI) for creating public key/private key pairs, checking for revocation, and performing other tasks. In addition, there must be a way to certify CAs as acceptable. (Certificate authorities are not regulated, and it is up to supply chains to determine which to trust.)

There are two final points about digital signatures. First, certificate authorities only vouch for a party’s public key. This does not mean that the party is trustworthy. That is a separate issue for supply chains to resolve. A reputation system could be developed for vendors in real ICATS systems.

Second, some certificate authorities offer a range of certification options from simply having an e-mail address to having the CA visit the company and inspect its physical status and its books. The highest form of certification reduces risk but does not eliminate them.
As part of a general risk control program, supply chains should carefully mandate minimum certification options.

For software, creating digital signatures is well established. Commercial products such as Tripwire create digital signatures for security purposes. If an attacker adds a virus to a program or replaces the program with a Trojan horse, the signature will change. However, as Tripwire users know, many programs change over time by their very operation. Specific versions of programs must be the targets of ICATS content authentication.

4. The ICATS tracking system

If verifiers work in a vacuum, many types of counterfeiting are difficult to stop. Consequently, ICATS would have a tracking system, as Figure 3 illustrates.

![Figure 3: ICATS tracking system](image)

As shown in the figure, there would be a central database for tracking a particular type of item. This database would be maintained by the producer or a trusted company to whom the producer outsources the maintenance work.

Whenever the item changes hands, information is uploaded to the database. The destruction of an item is also registered. This approach allows each verifier in the supply chain to determine the entire history of the item and to check for inconsistencies.

Ideally, the producer or outsourcer should actively look for signs of counterfeiting behavior, such as duplicate part numbers and odd patterns of part sales. In other words, ICATS should include or be used with a counterfeit detection system (CDS).

This detection functionality should be especially sensitive to indications of national adversary counterfeiting. In general, if discovered counterfeiting is very sophisticated, the counterfeiting detection system should issue a high-level alert (in ICATS terminology, a screech).

The tracking system should also accept input from verifiers that find or suspect that they find counterfeit parts. We include ‘suspect” because many parts are rejected after visual checking, but testing them to ensure true counterfeiting would be too expensive. The Department of Commerce [8] explicitly defines counterfeit parts as those what are proven or suspected to be counterfeit. Of course, this raises liability issues that need to be addressed.

Tracking systems can be maintained by suppliers or by the government. The choice is a political one and does not affect the technology. The presence of many ICATS databases, however, means that there should be central reporting databases to consolidate information (Item 7 in Figure 3). There already are multiple product deficiency tracking databases, including the Government-Industry Data Exchange Program (GIDEP), the Joint Deficiency Reporting System (JDRS), and the Product Data Reporting and Evaluation Program (PDREP). However, these are not directly focused on counterfeiting and have limited value in reducing counterfeiting risk. [10]. Ideally, this upgrading should allow them to accept input from multiple ICATSs and to do counterfeit-specific processing to identify trends.

The upgrading should also allow them to push out information to critical parties. For instance, if an ICATS query (sniff) would ask a central government database if a product under consideration has been reported to be problematic in a government database, the ICATS query response should list any counterindications for the product or specific serial number. In fact, government databases might push out lists of problem products and serial numbers to registered ICATSs.

5. Discussion

This paper outlines an approach (ICATS) to countering even the sophisticated counterfeiting that would be used by national advertisers to inject counterfeit hardware, software, or drugs into military
supply chains. This approach uses digital signatures and a tracking system to protect identity content contained on an item.

5.1 Potential benefits

The ICATS general approach offers three major advantages.

- First, public key encryption for authentication and identity content integrity is extremely strong cryptographically. Weaker authentication methods would increase risk.
- Second, the ICATS paw print concept does not limit the type or amount of identity content contained on the item. It is highly generalizable.
- Third, ICATS seems to be expensive, but something like it is done millions of times each day when browser users make online purchases under the protection of SSL/TLS. Browsers receive content protected by a digital signature and check the digital signature with a certificate authority. ICATs need not be prohibitively expensive.

5.2 Research directions

This paper has merely sketched the ICATS concept and hinted at extensions. To be useful, a great deal more research must be done on the concept and implementation details.

- As noted earlier, authentication is an endless cat and mouse game between impostors and verifiers. The research must identify possible attacks and develop countermeasures. Many countermeasures will be based on traditional overt and covert anti-counterfeiting methods used in the creation of paper money and product packaging. ICATS must be part of a larger anti-counterfeiting program.
- In addition, ICATS would only be one component in supply chain risk management. Research is needed in terms of how well ICATS will “play” with other countermeasures.
- Research is needed into the legal and organizational issues that need to be addressed to implement ICATS systems and use them successfully.
- Research is especially needed to estimate the cost of ICATs protection so that rational risk management analysis can compare costs with anticipated benefits. In shipping, there has been an effort since 2001 to add tamper-detection systems to shipping containers. However, a “conveyance security device” would cost about $2,500 per container, and this has been conserved prohibitively expensive by many. On the positive side, a comprehensive and automated tracking system may be able to reduce some of the business costs of supply chain management. If so, the ICATS concept could actually save money.

Once this initial research is done, a next logical step will be to define and create a prototype for proof-of-concept testing and cost estimation.

References