# Chapter 11
# Addressing Covert Channel Attacks in RFID-Enabled Supply Chains

**Kirti Chawla**
*University of Virginia, USA*

**Gabriel Robins**
*University of Virginia, USA*

## ABSTRACT

*RFID technology can help competitive organizations optimize their supply chains. However, it may also enable adversaries to exploit covert channels to surreptitiously spy on their competitors. We explain how tracking tags and compromising readers can create covert channels in supply chains and cause detrimental economic effects. To mitigate such attacks, the authors propose a framework that enables an organization to monitor its supply chain. The supply chain is modeled as a network flow graph, where tag flow is verified at selected key nodes, and covert channels are actively sought. While optimal taint checkpoint node selection is algorithmically intractable, the authors propose node selection and flow verification heuristics with various tradeoffs. The chapter discusses economically viable countermeasures against supply chain-based covert channels, and suggests future research directions.*

## 11.1 INTRODUCTION

Radio Frequency Identification (RFID) technology enables the tracking of objects via attached tags that respond to radio signals from readers (Finkenzeller (2003); Sweeney (2003)). Organizations can use RFID technology to streamline their internal processes and can optimize various phases of the production cycle, including asset management, inventory control, production tracking, shipping, recalls, and warranties (Angeles (2005); Min and Zhou (2002)).

However, the use of RFID technology can also leak sensitive information to adversaries about the internal processes of a target organization (Mitrokotsa, Reiback and Tanenbaum (2008)). For example, an adversary can track and/or modify tags, insert duplicate tags into supply chains, and

DOI: 10.4018/978-1-4666-3685-9.ch011

even compromise the RFID readers in the supply chain of a target organization. Such attacks "taint" the information flow, resulting in covert channels in the supply chain of a target organization (Moskowitz and Kang (1994)).

These covert channels can surreptitiously reveal product flow patterns, site-specific inventories, delivery schedules, and other strategic information. An adversary can use this illicitly obtained sensitive information to gain an unfair (and not necessarily even illegal) strategic or economic advantage with respect to a target organization. Given such possible threats, it is important for a target organization to control and verify the information flow in order to detect the presence of covert channels and mitigate their effect (Chawla, Robins and Weimer (2010)).

In this chapter, we analyze threat sources in RFID-enabled supply chains and focus on four representative attacks which adversaries can use to track the supply chains of target organizations. We consider the ability of such attacks to affect market change by modeling supply chains as network flow graphs, where nodes represent sites and edges model product flow. We designate key "taint checkpoint" nodes in the supply chain flow graph to verify the product information flow, and note that selecting such "taint checkpoints" optimally is NP-Complete.

We develop taint check cover heuristics based on tradeoffs, including the desired coverage (i.e. the number and locations of the desired taint checkpoints). We describe algorithms that verify the flow of information in the supply chain, both locally and globally. These algorithms offer user-controlled tradeoffs between the strength of the verification results versus the time required to compute them. This enables post-detection actions to be taken by the target organization, either at a local site or along selected global paths. Finally, we evaluate these approaches using a supply chain simulator, and provide remedies that target organizations can utilize to mitigate the impact of covert channels.

## 11.2 BACKGROUND

Supply chains are a collection of organizational processes spanning multiple geographic sites for the purpose of transforming raw materials into finished products, and delivering them from producers to consumers. Due to the large size and complexity of a typical supply chain, it is difficult to track and maintain cross-site inventories. Furthermore, mishaps such as loss or theft of products can cause serious financial losses to the organizations operating these supply chains. Products affixed with RFID tags can be tracked and queried universally at any place and time. Thus, with the advent of RFID technology, supply chains are becoming more efficient in managing inventories and preventing theft (Niederman, Mathieu, Morley and Kwon (2005); Wilding and Delgado (2004)).

However, such flexibility also gives rise to novel spatial-temporal inferences through embedded covert channels that could reveal product flow patterns within supply chains. While this technology is critical to the smooth functioning of a target organization, it may also leak sensitive information to competitors who may unscrupulously leverage it to affect market changes. To remain economically viable, target organizations must actively mitigate the adversarial impact of covert channels on its profitability and economic competitiveness.

## 11.3 THREATS IN RFID-ENABLED SUPPLY CHAINS

To analyze potential threats to RFID-enabled supply chains, we present a threat model and focus on four possible supply chain attacks.

### 11.3.1 Threat Model

The proposed threat model uses a motivating example to highlight the underlying key assumptions. Consider two competing businesses that develop ubiquitous and interchangeable products (e.g. cellular phones). Such businesses use competitive pricing and features as key differentiating factors, tailoring their products according to brand loyalties and user preferences. Assume that both businesses are competing for the same consumer base in the same markets, and are striving to make their supply chains more efficient by optimizing their internal processes. Often the target business invests in new technology, such as RFID, after performing appropriate cost-benefit analyses. While the benefits may be immediately evident (e.g., efficient inventory control, real-time production tracking, speedy warranty authorizations, etc.,) the cost of utilizing such a technology may involve more than just the direct cost of installing RFID equipment and processes.

In order to remain competitive, the adversary business may also adopt RFID technology. Moreover, the adversary can also exploit this technology to fraudulently learn patterns of product flow in the supply chain of the target business. Such patterns can be used in time-sensitive ways to provide lower consumer prices, or flood the adversary's products into selected regions or stores while the products of the target business become scarcer.

Such practices can be construed as industrial or economic espionage and can significantly reduce the profitability of the target business. The resulting profit drop can be viewed as a hidden cost that would be difficult to anticipate or even identify by the target business. Moreover, recent advances in RFID technology and its wide-spread use can provide adversaries with selective "insider access" of target businesses' supply chains, without requiring direct access to their physical premises.

### 11.3.2 Possible Attacks

Supply chains of target organizations can unintentionally reveal product flow patterns to adversaries in a number of ways. We enumerate four representative attacks (see Figure 1), some of which have already received attention from the security research community (Avoine, Lauradoux and Martin (2009); Juels, A., Rivest, R.L., and Szydlo, M. (2003); Koscher, Juels, Brajkovic and Tadayoshi (2009); Mandel, Roach and Winstein (2004); Mitrokotsa, Reiback and Tanenbaum (2008); Weis, S. A. et al. (2004)). We explain the significance of these attacks when applied to a supply chain scenario, discuss the potential implications, and present possible ways to mitigate such attacks. While the proposed attacks can be executed over any given RFID standard, this chapter assumes the *EPC Gen2* RFID standard (EPCGlobal (2008); EPCGlobal (2011)). The following types of attacks create covert channels that are said to "taint" the supply chain of a target organization.

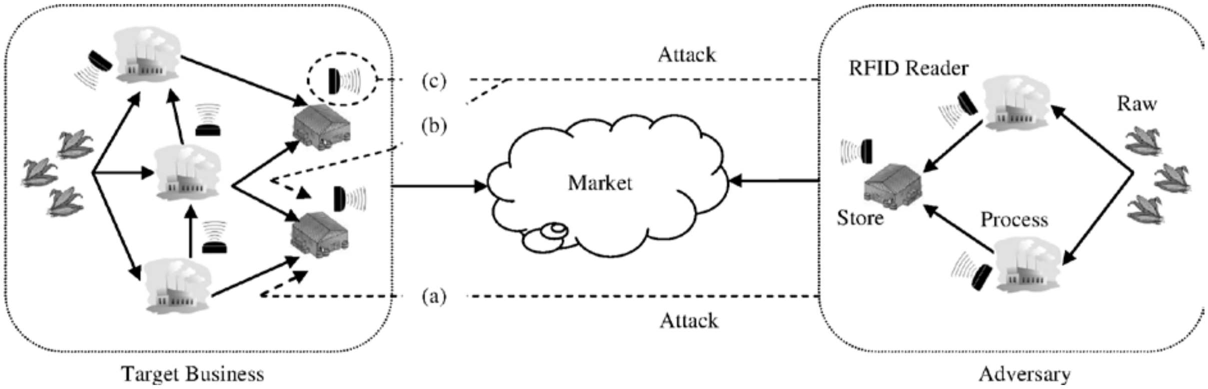
#### Attack 1: Tag Tracking

In this attack, an adversary tracks existing tags across the supply chain of a target business. Such tags can be applied at the product-level or case-level. We assume that a target business assembles the finished product at its factory, attaches the tags at the case-level, and then ships cases to geographically -separate warehouses. These cases are eventually organized into different batches and delivered to various retail stores. An adversary can learn the product flow patterns by copying the information stored in some case-level tags, and then querying them at different places in the supply chain (e.g. by deploying long-range readers). Such copied case-level tags constitute a covert channel, as they leak product flow information to the adversary, while traveling unobtrusively through the supply chain of the target business.

#### Attack 2: Tag Duplication

In this attack, an adversary copies the information stored in an existing tag and constructs a duplicate tag. Consequently, the adversary can attach this duplicate tag to a different case, enabling it to become part of the supply chain of the target

*Figure 1. (a) Inserting duplicate tags, (b) modifying existing tags, and (c) compromising existing readers*



business and thus, a covert channel. The adversary then queries the cases at different points of the supply chain to determine the product flow (i.e. if the adversary sees two duplicate case-level tags at a warehouse then he can infer that they aggregated at that warehouse after originating from different locations). This attack scenario is more powerful than the previous tracking-only attack, since here the adversary can still track legitimate supply chain tags as well as its own surreptitiously inserted duplicated tags. An adversary can mount such an attack with modest effort, since tag duplication hardware is relatively inexpensive and easily available (Mandel, Roach and Winstein (2004)).

## Attack 3: Tag Modification

In an *EPC Gen2*-compliant tag, there are four memory banks: *EPC*, *TID*, *User*, and *Reserved*. While the inventory process of a target business supply chain primarily uses the EPC portion of a tag's memory, the contents of the other memory banks are ignored. Therefore, an adversary can modify the information in the writable portions of other memory banks, which can then serve as a covert channel. Independently, it has been suggested that the unused portion of memory of a tag can be utilized to conceal information (Karygiannis, Phillips, and Tsibertzopoulos (2006); Mitrokotsa, Reiback and Tanenbaum (2008)). Such a vulnerability can be an attractive target to an adversary, due to its potentially large payoff versus the relatively low effort required to exploit it.

## Attack 4: Reader Compromise

With rapid advances in RFID technology, RFID readers are available in a variety of form-factors, hardware/software combinations, and use-case scenarios (e.g., rack-mountable, battery-powered, etc.). Many of these readers are deployed in supply chains in a manner that enables an adversary to compromise them (e.g., snooping on a wireless reader transmission, compromising the on-board software or hardware of a mobile reader, etc.).

In Figure 2 (a), a compromised reader copies information stored in several case-level tags, and provides it to an adversary. In Figure 2 (b), an adversarial compromised reader selectively repudiates (i.e. intentionally fails to report) the presence of any duplicate or modified tags. Such compromised views from the readers enable covert channels to exist unobtrusively in the supply chains of target organizations.

We note that such a reader-compromise attack subsumes the tag duplication and modification attacks in terms of potential risks to the target organization. From the adversary's perspective, in order to ensure a successful attack, while at least one compromised tag at the case-level is necessary, it may not be sufficient, since that tag may fail or become undetectable. Thus, several compromised (i.e. duplicated and/or modified) tags should be used at the case-level (say, at least three tags per 100 cases). On the other hand, if too many compromised tags (i.e. half of the total) are deployed, the adversary's exposure risk also increases dramatically. Moreover, an adversary may not need to track product flow information at the product-level, since case-level tracking is sufficient for that purpose.

### 11.3.3 Market Change Scenarios

We examine two possible market scenarios to illustrate the potential harmful impact of the RFID-based attacks described above. A typical supply chain involves business-related variables such as inventory levels at factories and retailers, delivery schedules from raw material sites to warehouses, shipping capabilities, backlog of orders, etc. Leaks of such strategic business information can occur via attacks on supply chains, which can enable an adversary to engage in unfair competitive practices. Furthermore, an adversary can affect negative market changes by knowing the business practices of its competitors. We used the *Anylogic* supply chain model simulator (Anylogic (2009)) to generate economic impact projections and qualitatively outline possible outcomes of such attacks.

### Case 1: Brand Loyalty Change

In the first scenario (Figure 3), we consider two businesses serving a population of 10,000 consumers with brands A and B, respectively. We assume that the two brands are interchangeable, and have the same retail price. The business with brand B is the target business, while the business with brand A is the adversary. Consumers must purchase either brand A or brand B per time unit (i.e. the product is a staple product).

In Figure 3 (a), consumers are projected to prefer brand B to brand A by 55% to 45% (i.e. whenever a consumer arrives at a store, he chooses a product at random from the set of available equivalent products, preferring brand B slightly over brand A). However, by carefully timing its production so that more brand A products are available at a time when fewer brand B products are available, an adversary can induce consumers to switch brands. In Figure 3 (b), the

*Figure 2. Reader compromise attack: (a) copy case-level tags, and (b) repudiate the presence of a covert channel*

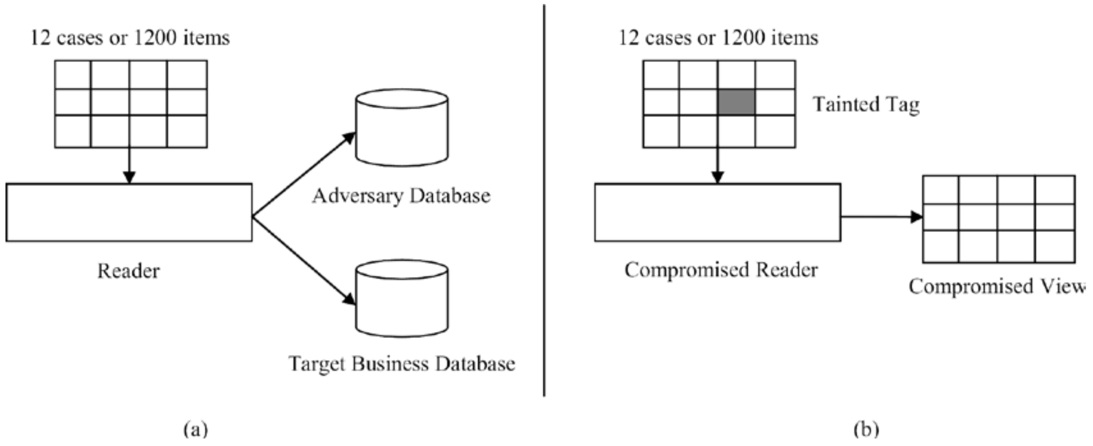
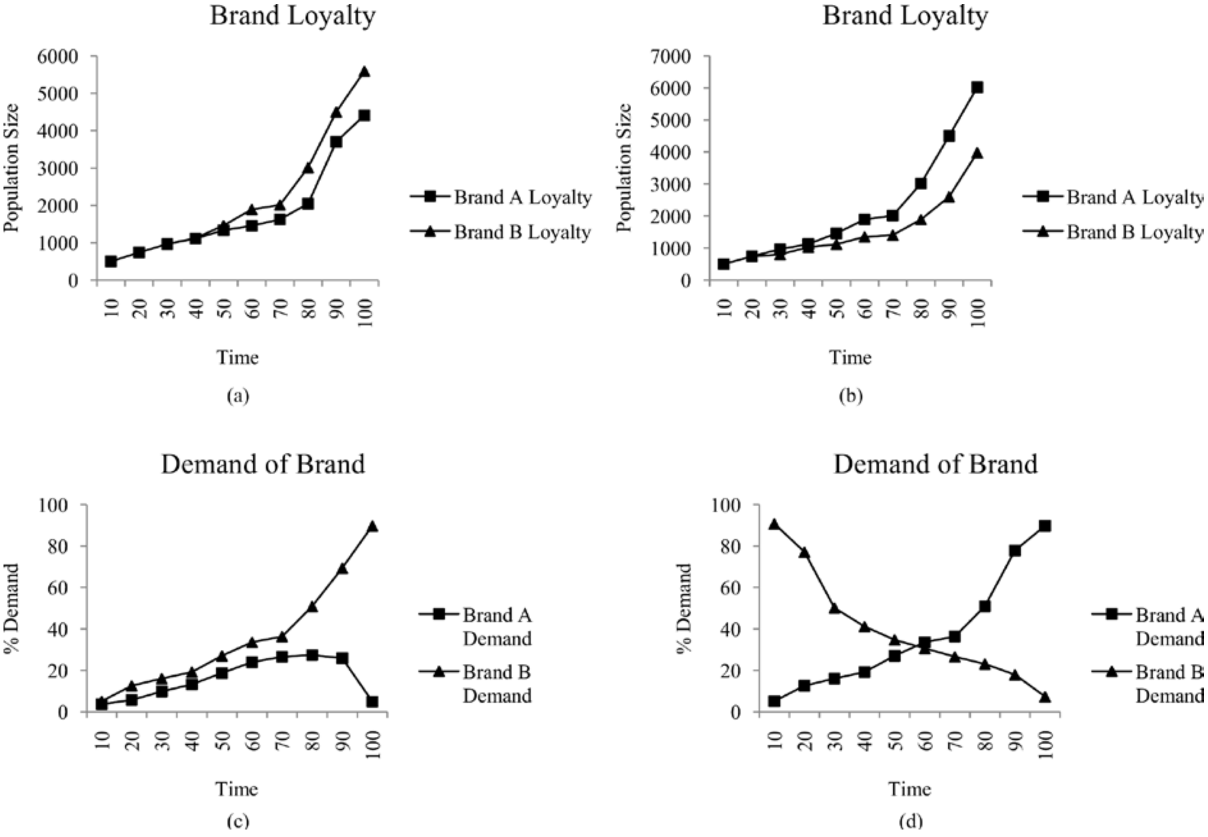


*Figure 3. Market change projections using the anylogic supply chain simulator (Anylogic 2009): (a) consumers prefer brand B over brand A, (b) consumers switch from brand B to brand A, (c) brand B enjoys more demand than brand A, and (d) brand A demand increases, while brand B demand decreases*



adversary has succeeded in inducing the consumers to switch brands, now favoring A over B by 57% to 43%.

## Case 2: Brand Aversion

In the second scenario (Figure 3), we consider a neighborhood store served by two businesses A and B, as described above. Stores often stock products that enjoy consistent demand, in order to maintain profitability. Initially, the store stocks both products in equal amounts. However, at a later time, as shown in Figure 3 (c), brand B (i.e. product of the target business) is projected to have a higher demand than brand A by 89% to 5%. There is typically a demand threshold below which it will become non-profitable to stock a brand (i.e. leading to "brand aversion"). An adversary aiming to bolster its own shelf presence may resort to illegitimately acquiring sensitive supply chain information of the target business. Figure 3 (d) depicts such a scenario, where the adversary engages in supply chain attacks to obtain time-sensitive information about a target business, and uses that information to manipulate the market.

## Observations for Market Change Scenarios

Augmenting a supply chain with RFID technology entails attaching RFID tags at the product-level or case-level, and then tracking them throughout the supply chain using RFID readers. The target business keeps track of products starting from the purchase phase (i.e. as raw materials) through the distribution phase (i.e. as finished products stored at warehouses or retail outlets). An adversary can use the possible attacks described above in order to learn vital strategic information, resulting in the projected market change scenarios, to the detriment of the target business.

If the potential benefits outweigh the incurred costs, adversaries have strong motivation (i.e. economic incentive) for perpetrating such attacks. Thus, such attacks are viable in an RFID-enabled supply chain given the potentially high payoff to an adversary, although specific occurrences of such attacks seem to have not yet been publicly reported. While we have argued that the exposure of only a few business variables to an adversary can result in an unfair (and not necessarily even illegal) marketplace economic advantage, it would be interesting to study more elaborate and detailed marketplace scenarios and projections. Such possible scenarios can stimulate further discussions regarding the associated risks as well as the effectiveness of possible solutions in RFID-enabled supply chains.

## 11.4 SUPPLY CHAIN MODEL

We now focus on the problem of modeling a supply chain, towards the goals of preventing covert channel attacks and mitigating their effects. A supply chain typically spans multiple geographically separate sites and involves numerous phases that include the sourcing of raw materials, processing and storing end-products, and delivering these products to markets and consumers. Supply chain models can be categorized as deterministic models, stochastic models, hybrid models, economic models, and IT driven models (Angeles (2005); Min and Zhou (2002); Swaminathan, Smith and Sadeh (1998)). While these models aim to capture many aspects of a supply chain in great detail, our goal is to construct a simpler model that will enable us to focus on the fundamental issues related to potential covert channel attacks.

In a supply chain, there are product flows between sites (i.e. raw materials moving among various locations). In an RFID-enabled supply chain, however, product flow between sites is analogous to "tag-flow", since RFID tags are attached to each product. The supply chain consists of multiple phases, wherein each phase is a collection of sites. Furthermore, to detect the presence of duplicate tags, modified tags, or compromised readers, we need mechanisms to track product flow between supply chain phases. With these three key observations in mind, we developed a model based on network flow graphs (Cormen, Leiserson, Rivest and Stein (2009)), called "supply chain flow graphs."

### 11.4.1 Logistical Phases

A supply chain typically spans three phases: the purchase phase, the production phase, and the distribution phase (e.g. sites associated with the production phase are involved primarily in manufacturing a product). Each phase of the supply chain is a collection of interconnected sites having product flows among them. We define the supply chain flow graph $G = (V, E)$ as a directed, connected graph, where a node $p$ corresponds to a site, and an edge $(p, q)$ models a product flow between the two sites. Each edge $(p, q) \in E$ has a positive product flow capacity $C(p, q) > 0$, while "non-edges" have no capacity (i.e. $\forall\ (p, q) \notin E$, $C(p, q) = 0$). There are two special nodes called the "source node" ($S$) and the "sink node" ($T$). We partition the supply chain flow graph into three sub-graphs, corresponding to the purchase phase, production phase, and distribution phase, respectively (other more specialized supply chains may contain additional phases).

Network flows are subject to the usual constraints on edge capacity and flow conservation at nodes (Cormen, Leiserson, Rivest and Stein

(2009)). We propose an additional property, namely the node maximal outgoing flow, which will enable us to address issues related to attacks. There are typically multiple paths for product flow in a supply chain. A "critical node" or "critical edge" may experience more product flow than those along other paths. We model such supply chain characteristics by keeping track of each node's maximum outgoing flow. If two nodes have the same maximal outgoing flow, we resolve the tie by giving precedence to the node having a predecessor with a higher flow value. Supply chain flow graphs having such critical paths facilitate reasoning about issues related to possible attack locations and product flow inspection sites.

## 11.4.2 Taint Checkpoints

A direct approach for detecting covert channel attacks may require looking for tainted RFID tags at every node of the supply chain. However, this would be prohibitively expensive and time consuming. Instead, we propose to select a subset of nodes, called "taint checkpoints", verify the product flow at these selected locations, and report the presence of any discovered covert channels in the supply chain flow graph. When RFID tags are attached to products by the target business in the early phases of the supply chain, the information onboard the tags is recorded in order to track the inventory.

In subsequent phases of the supply chain, this information is available to taint checkpoints for the purpose of inspection and verification. This verification process involves comparing the information present onboard a currently viewable RFID tag with the trusted and previously stored information. Any mismatch may indicate the presence of covert channels or other tampering. Figure 4 illustrates a supply chain flow graph, including several taint checkpoints where product flow is inspected.

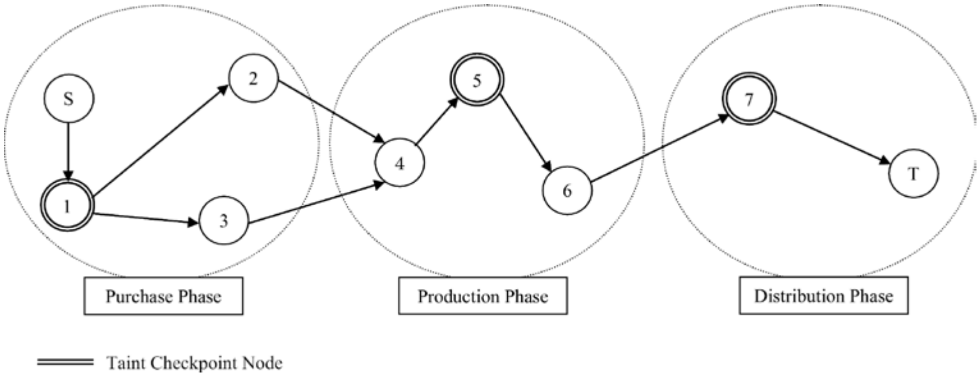
## 11.4.3 Taint Checking and Verification Algorithms

Based on the above observations, we formulate the problem of optimally selecting taint checkpoints in the supply chain flow graph. We show that this problem is NP-Complete (i.e. computationally intractable), and suggest heuristics to generate good approximate solutions.

### Problem Statement: Taint Check Cover

To ensure the absence of covert channels in the supply chain, the taint checkpoints should provide broad coverage for the entire graph. The related optimization problem is to select as few taint checkpoints as possible, while providing broader coverage for the entire supply chain flow graph. Thus, we seek a "taint check cover" *V'* of the

*Figure 4. A supply chain flow graph with three taint checkpoints*



supply chain flow graph $G = (V, E)$, where $V' \subseteq V$, such that every edge of $E$ has at least one of its end points (i.e. nodes) in $V'$. Note that we may choose to only cover some critical node subset of the supply chain flow graph rather than the entire graph. Either way, this objective corresponds to the classical graph vertex cover problem, which is known to be NP-complete (Cormen, Leiserson, Rivest and Stein (2009)).

## Heuristic Taint Check Cover Generation

There is a known efficient heuristic for the vertex cover problem that produces solutions of size no worse than twice the optimal (Cormen, Leiserson, Rivest and Stein (2009)). This heuristic selects an arbitrary graph edge, adds its two end points to the growing vertex cover solution, eliminates this edge and its end points from the graph, and iterates until the entire graph is exhausted. To see that this scheme produces a worst-case twice-optimal solution, we observe that at least one of the two nodes of each removed edge must be present in any optimal solution.

Given the high degree of freedom in how edges (and thus nodes) are selected in constructing such a heuristic taint check cover solution, a target business may introduce different selection criteria, based on practical, economic, or strategic considerations. A target business may wish to limit the number of taint checkpoints, or balance the cost of its supply chain versus the coverage provided by the taint checkpoints. On the other hand, we may also consider taint checkpoint selection criteria based on the specific structure of the supply chain, or some other combination based on these considerations. To address these factors, we give several possible formulations of the supply chain flow graph coverage problem as follows:

- **Maximum Edge Cover:** Given a supply chain flow graph $G$ and an integer $K$, find a taint check cover (node set) of size $K$ having a maximum total number of adjacent edges.
- **Minimum Taint Checkpoint Cover:** Given a supply chain flow graph $G$ and an integer $J$, find a minimum taint check cover (node set) with at least $J$ total adjacent edges.

These formulations naturally generalize to scenarios where, as part of the input, we also designate a given subset of the nodes or edges (or both nodes and edges) that must be included in the taint check cover. When determining a taint check cover, the target business may choose from a continuous tradeoff between infrastructural costs and overall taint check coverage. This can be accomplished using greedy approaches such as the 2 ·OPT node cover heuristic (Cormen, Leiserson, Rivest and Stein (2009)) discussed above, the techniques described in (Chen, Kanj and Jia (2001); Niedermeir and Rossmanith (1999)), or any other taint check cover heuristic.

Alternatively, nodes can be selected by decreasing order of maximal outgoing flow values, in order to give higher priority to high-flow nodes. Furthermore, we can utilize the classical min-cut-max-flow theorem (Cormen, Leiserson, Rivest and Stein (2009)) and preferentially select high-flow nodes along some minimum cut. This will tend to maximize the overall probability of detecting covert channels (which must cross any graph cut). Moreover, the nodes may be permuted in some other manner (e.g., by aggregate product value, time-criticality, geographical distribution, or even randomly), in order to capture topological or economic considerations. In summary, our algorithmic template is quite general and can utilize many alternative possible criteria to construct taint check covers.

Note that not every node and edge in the flow graph must necessarily be covered, since tainted tags that are missed at some points along the graph will likely be discovered at subsequent downstream locations. On the other hand, including any flow graph "cut" in the taint check cover ensures that every tainted tag will *eventually* be discovered in at least one location. Toward this goal, cuts containing smaller number of nodes are more efficient than larger node cuts (i.e. they will require fewer readers at taint checkpoints to achieve the same guaranteed taint checking coverage). Choosing small (or even optimal) graph cuts can be accomplished using known min-cut algorithms (Stoer and Wagner (1997)). Figure 4 illustrates a cut-based cover utilizing phase criteria for a sample supply chain flow graph.

### Verification Algorithm

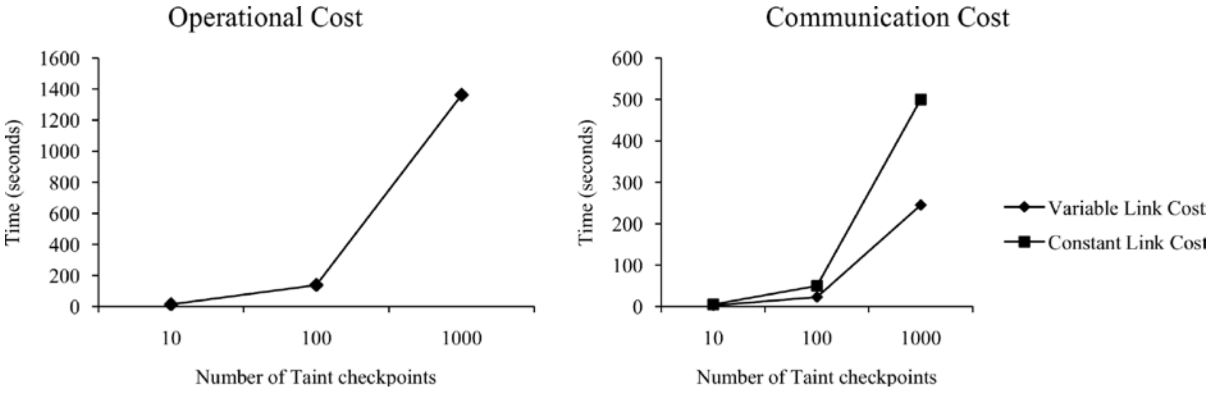
Each node (i.e. a taint checkpoint) in the taint check cover is responsible for inspecting and verifying the product flow passing through it. Each product in this flow has a unique RFID tag ID. If a taint checkpoint reads multiple counts of the same tag ID, or the system detects the same tag ID at two different places simultaneously, then a duplicate tag has been detected. By comparing the information present onboard each viewable tag with data stored a priori in a trusted backend database, modifications to tags can be detected at taint checkpoints. We note that such product flow verifications can be performed "locally" at a given taint checkpoint or "globally" across a given path or cut, as taint checkpoints accumulate, exchange, and compare tag information.

## 11.5 EVALUATION AND ANALYSIS

We used simulations to evaluate our proposed approaches. We randomly constructed a base supply chain flow graph configuration of 2000 nodes and selected among 10, 100, and 1000 nodes to be taint checkpoints. Each checkpoint is assumed to be able to verify 1000 cases of 100 units of product at each time interval. We assume each taint checkpoint has direct access to the trusted database implementing a tag lookup service. In our first simulation, we measured the relationship between the number of taint checkpoints and the cumulative time required to perform local verification (i.e. the maximum reading rate of the RFID readers).

Figure 5 (a) shows that as the number of taint checkpoints increases, there is a corresponding increase in the time to locally verify the product flow. Our second simulation evaluates the global verification algorithm, which collects local verification results from taint checkpoints. The cost of the collection process depends on the underlying bandwidth of the network links. Figure 5 (b) shows the simulated verification cost when the link cost is either constant (500 ms), or a variable (ranging from 2 to 1000 ms) time window proportional to the geographical distance of the taint checkpoints from the central database server.

*Figure 5. (a) Cumulative local verification time as a function of the number of taint checkpoints, and (b) local and global verification costs as a function of the number of taint checkpoints*



Thus, we explored the verification communication cost as the number of taint checkpoints increases. We observed that the communication cost can grow rapidly in a more realistic scenario where taint checkpoints are at larger variable distances from the check nodes.

## 11.6 RESPONSES TO COVERT CHANNELS

We enumerate several possible mitigating techniques available to the target organizations when the covert channels are detected in their supply chains. Note that the presence of covert channels in the supply chain can never be completely ruled out, even when privacy-preserving algorithms are used in the underlying RFID technology (Bailey, Boneh, Goh and Juels (2007); Garfinkel, Juels and Pappu (2005)).

### 11.6.1 Response 1: Authentication

According to the *EPC Gen2* RFID standard, an RFID tag is required to support password protection for read or write access to the tag. The systematic use of passwords can mitigate tag tracking, duplication, and modification attacks. However, this technique requires that the RFID system in the supply chain support and conform to the chosen password schemes. Alternatively, challenge-response based authentication protocols can be used to thwart tag tracking, modification and duplication attacks (Rhee, Kwak, Kim and Won (2005)). Moreover, compromised readers may be authenticated with respect to genuine tags using a technique described in (Paise and Vaudenay (2008)).

### 11.6.2 Response 2: Pseudonym

An RFID tag using pseudonyms transmits a slightly different ID each time it is queried (Molnar, Soppera and Wagner (2005)). This can prevent the adversary from discovering patterns in a supply chain, but requires the target business to accommodate a pseudonym scheme in its tracking logic. Also, (Burmester and Munilla (2009)) describe an unlinking technique that can be used to prevent tag tracking attacks. Additionally, blocker tags can be utilized to selectively block compromised readers (Juels, Rivest and Szydlo (2003)).

### 11.6.3 Response 3: Re-Encryption

The use of encryption to conceal the tag's data can still allow an adversary to track a statically encrypted tag over the supply chain. To defeat such an attack, the tags can be re-encrypted after each phase of the supply chain, in order to prevent the adversary from modifying or tracking the tags. Techniques described in (Golle, Jakobsson, Juels and Syverson (2004); Saito, Ryou, and Sakurai (2004)) can be used to anonymize tags via re-encryption.

### 11.6.4 Response 4: Direct Mitigation

The work of (Reiback, Crispo and Tanenbaum (2005)) describes a device that can be used for sweeping and preventing reader compromise attacks. When a covert channel source is discovered, an operator can physically clear the operating environment while temporarily altering the flow of products. Alternatively, path checking techniques can trace tags that follow altered routes (Oua and Vaudenay (2009)). Furthermore, physically detaching a tag's body from its antenna (temporarily) can serve as an effective (albeit cumbersome) technique to prevent RFID-based attacks en route between supply chain sites (Karjoth and Moskowitz (2005)).

### 11.6.5 Response 5: Physically Unclonable Functions (PUF)

Physically unclonable functions (PUFs) are easy to evaluate but hard to characterize or duplicate. For example, PUFs may be used to generate random numbers based on the variability inherent in the manufacturing processes of the underlying VLSI circuits (Bolotnyy and Robins (2007)). PUF-based privacy-preserving algorithms can provide a way to build message authentication codes to ensure data integrity and aid in preventing tag modification attacks.

## CONCLUSION

We discussed and analyzed vulnerabilities in RFID-enabled supply chains, and enumerated possible attacks that can be perpetrated with relatively modest effort. An adversary can thus surreptitiously learn product flow patterns in the RFID-enabled supply chain of a target organization, which may result in privacy leakage and economical damage. We proposed a simple model for reasoning about supply chain flow and RFID attack mitigation, and demonstrated that attacks can be detected and addressed at selected nodes in a supply chain. We presented a practical heuristic template for the computationally intractable problem of optimal taint checkpoint selection that enables trading off protection coverage against overall cost. We simulated and analyzed verification algorithms, and enumerated several possible responses against detected covert channels.

This chapter represents an important step toward the analysis and mitigation of attacks on RFID-enabled supply chains. We envision that the proposed basic supply chain model can be extended to include additional practical considerations (e.g., multi-product supply chains, adversary cartels, cost-benefit analyses, supply chain topology-specific constraints, fine-grained product flow analyses, market change scenarios, etc.) such as described in (Lee and Whang (2005)). Future heuristics may be fine-tuned to address such additional practical considerations. Finally, it would be interesting to further study the comparative tradeoffs between coverage, cost, and efficiency for different taint checkpoint selection strategies in realistic scenarios.

## ACKNOWLEDGMENT

This research was supported by National Science Foundation (NSF) grant CNS-0716635.

## REFERENCES

Angeles, R. (2005). RFID technologies: Supply-chain applications and implementation issues. *Information Systems Management*, *22*(1), 51–65. doi:10.1201/1078/44912.22.1.20051201/85739.7

Anylogic Professional 6. (2009). *AB-SD supply chain model simulator*. Retrieved from http://www.xjtek.com

Avoine, G., Lauradoux, C., & Martin, T. (2009). Lecture Notes in Computer Science: *Vol. 5932*. *When compromised readers meet RFID. Information Security Applications* (pp. 36–50). Springer. doi:10.1007/978-3-642-10838-9_4

Bailey, D. V., Boneh, D., Goh, E., & Juels, A. (2007). Covert channels in privacy-preserving identification systems. *14th ACM International Conference on Computer and Communication Security*, (pp. 297-306).

Bolotnyy, L., & Robins, G. (2007). Physically unclonable function-based security and privacy in RFID systems. *5th International Conference on Pervasive Computing and Communications*, (pp. 211-120).

Burmester, M., & Munilla, J. (2009). *A flyweight RFID authentication protocol.* Workshop on RFID Security.

Chawla, K., Robins, G., & Weimer, W. (2010). On mitigating covert channels in RFID-enabled supply chains. *Radio Frequency Identification System Security (RFIDsec), Workshop on RFID Security*, (pp. 135-146).

Chen, J., Kanj, I. A., & Jia, W. (1999). Vertex cover: Further observations and further improvements. *Journal of Algorithms*, *41*, 313–324.

Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2009). *Introduction to algorithms* (3rd ed.). MIT Press.

EPCGlobal. (2008). *UHF C1 G2 air interface protocol standard*. Retrieved from http://www.epcglobalinc.org/standards/uhfc1g2/uhfc1g2_1_2_0-standard-20080511.pdf

EPCGlobal. (2011). *Tag data standards version 1.6*. Retrieved from http://www.gs1.org/gsmp/kc/epcglobal/tds/tds_1_6-RatifiedStd-20110922.pdf

Finkenzeller, K. (2003). *RFID-handbook: Fundamentals and applications in contactless smart cards and identification* (2nd ed.). Munich, Germany: Wiley and Sons Inc.

Garfinkel, S. L., Juels, A., & Pappu, R. (2005). RFID privacy: An overview of problems and proposed solutions. *IEEE Security and Privacy*, *3*(3), 34–43. doi:10.1109/MSP.2005.78

Golle, P., Jakobsson, M., Juels, A., & Syverson, P. (2004). Lecture Notes in Computer Science: *Vol. 2964*. *Universal re-encryption for mixnets. Topics in Cryptology - CT-RSA 2004* (pp. 163–178). Springer. doi:10.1007/978-3-540-24660-2_14

Juels, A., & Pappu, R. (2003). Lecture Notes in Computer Science: *Vol. 2742*. *Squealing Euros: Privacy protection in RFID-enabled banknotes. Financial Cryptography* (pp. 103–121). Springer. doi:10.1007/978-3-540-45126-6_8

Juels, A., Rivest, R. L., & Szydlo, M. (2003). The blocker tag: Selective blocking of RFID tags for consumer privacy. *10th ACM Conference on Computer and Communications Security*, (pp. 103-111).

Karjoth, G., & Moskowitz, P. A. (2005). Disabling RFID tags with visible confirmation: Clipped tags are silenced. *ACM Workshop on Privacy in the Electronic Society*, (pp. 27-30).

Karygiannis, A., Phillips, T., & Tsibertzopoulos, A. (2006). RFID security: A taxonomy of risks. *Conference on Communications and Networking in China*, (pp. 1-8).

Koscher, K., Juels, A., Brajkovic, V., & Tadayoshi, K. (2009). EPC RFID tag security weaknesses and defenses: Passport cards, enhanced drivers licenses, and beyond. *16th ACM Conference on Computer and Communications Security*, (pp. 33-42).

Lee, H. L., & Whang, S. (2005). Higher supply chain security with lower cost: Lessons from total quality management. *International Journal of Production Economics*, *96*, 289–300. doi:10.1016/j.ijpe.2003.06.003

Mandel, J., Roach, A., & Winstein, K. (2004). *MIT proximity card vulnerabilities*. MIT Technical report. Retrieved from http://web.mit.edu/keithw/Public/MIT-Card-Vulnerabilities-March31.pdf

Min, H., & Zhou, G. (2002). Supply chain modeling: Past, present and future. *Journal of Computer and Industrial Engineering*, *43*(1-2), 231–249. doi:10.1016/S0360-8352(02)00066-9

Mitrokotsa, A., Rieback, M. R., & Tanenbaum, A. S. (2008). Classification of RFID attacks. *International Workshop on RFID Technology*, (pp. 73-86).

Molnar, D., Soppera, A., & Wagner, A. (2005). Lecture Notes in Computer Science: *Vol. 3897*. *A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags. Selected Areas in Cryptography* (pp. 276–290). Springer. doi:10.1007/11693383_19

Moskowitz, I. S., & Kang, M. H. (1994). Covert channels here to stay. *9th IEEE International Conference on Computer Assurance*, (pp. 235-243).

Niederman, F., Mathieu, R. G., Morley, R., & Kwon, I. (2005). Examining RFID applications in supply chain management. *Communications of the ACM*, *50*(7), 93–102.

Niedermeir, R., & Rossmanith, P. (1999). Upper bounds for vertex cover further improved. *16th Symposium on Theoretical Aspects in Computer Science, Lecture Notes in Computer Science, Vol. 1563,* (pp. 561-570). Springer.

Orlin, J. B. (1988). A faster strongly polynomial minimum cost flow algorithm. *20th ACM Symposium on Theory of Computing*, (pp. 377-387).

Oua, K., & Vaudenay, S. (2009). *Pathchecker: An RFID application for tracing products in supply-chains*. Workshop on RFID Security.

Paise, R., & Vaudenay, S. (2008). Mutual authentication in RFID. *3rd ACM ASIA Conference on Computer and Communications Security*, (pp. 292-299).

Rhee, K., Kwak, J., Kim, S., & Won, D. (2005). Lecture Notes in Computer Science: *Vol. 3450. Challenge-response based RFID authentication protocol for distributed database environment. Security in Pervasive Computing* (pp. 70–84). Springer. doi:10.1007/978-3-540-32004-3_9

Rieback, M. R., Crispo, B., & Tanenbaum, A. S. (2005). Lecture Notes in Computer Science: *Vol. 3574. RFID guardian: A battery-powered mobile device for RFID privacy management. Information Security and Privacy* (pp. 184–194). Springer.

Saito, J., Ryou, J. C., & Sakurai, K. (2004). Lecture Notes in Computer Science: *Vol. 3207. Enhancing privacy of universal re-encryption scheme for RFID tags. Embedded and Ubiquitous Computing* (pp. 879–890). Springer. doi:10.1007/978-3-540-30121-9_84

Stoer, M., & Wagner, F. (1997). A simple min-cut algorithm. *Journal of the ACM*, *44*(4), 585–591. doi:10.1145/263867.263872

Swaminathan, J. M., Smith, S. F., & Sadeh, N. M. (1998). Modeling supply chain dynamics: A multiagent approach. *Decision Sciences*, *29*(3), 607–632. doi:10.1111/j.1540-5915.1998.tb01356.x

Sweeney, P. J. (2005). *RFID for dummies*. Wiley Publishing, Inc.

Weis, S. A., Sarma, S. E., Rivest, R. L., & Engels, D. W. (2004). Lecture Notes in Computer Science: *Vol. 2802. Security and privacy aspects of low-cost radio frequency identification systems. Security in Pervasive Computing* (pp. 201–212). Springer.

Wilding, R., & Delgado, T. (2004). RFID demystified: Supply chain applications. *Logistics and Transport Focus*, *6*(4), 42–47.

## KEY TERMS AND DEFINITIONS

**Flow Network:** In graph theory, a flow network models the movements of commodities using a weighted graph, where edges have associated maximum capacities, and the total incoming/outgoing flow at each node is conserved.

**Market Change Scenario:** A change in the underlying dynamics of a market involving supply, demand, consumption, businesses, competition, and consumers.

**Maximal Outgoing Flow:** A node's property in a flow network where the edge having the maximum flow value among the number of outgoing edges is selected in order to identify the critical path.

**NP-Complete:** A class of problems in computational complexity theory that are likely to be intractable (i.e. not likely to be solved deterministically within polynomial time).

**Pseudonym:** An RFID tag ID that changes each time the tag is read.

**PUF:** Physically Unclonable Function is a function that is easy to evaluate but hard to characterize or duplicate. For example, PUFs may be implemented aboard RFID tags based on the manufacturing variability inherent to the underlying electronic circuits.

**Re-Encryption:** The process of iteratively composing multiple encryptions of data (onboard a tag), which can vary based on time and location.

**RFID:** Radio Frequency Identification is a radio-based technology that can be used to track and identify tagged objects.

**Supply Chain:** A supply chain is a system of processes, organizations, technology, activities, information, resources, and people that move products from producers to consumers.

**Taint Check Cover:** A minimum set of nodes that cover (i.e. are adjacent to) all the edges of the supply chain flow graph.

**Taint Check Point:** A node in the taint check cover set.